**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені ІГОРЯ СІКОРСЬКОГО»**
Факультет електроніки
(повна назва інституту/факультету)

Кафедра звукотехніки та реєстрації інформації
(повна назва кафедри)

«На правах рукопису»
УДК 621.397.63

«До захисту допущено»

Завідувач кафедри
_____ __Г.Г. Власюк_
(підпис) (ініціали, прізвище)

“_9_” ___грудня___2019 р.

# Магістерська дисертація

спеціальність 171 «Електроніка»
(код і назва)

на тему: «Система забезпечення безпеки із застосуванням технології IoT»

Виконав: студент II курсу, групи ДВ-82мп
(шифр групи)

Наровський Олексій Михайлович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник доцент, к.т.н., доцент Лазебний В. С. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____
(науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада,науковий ступінь,вчене звання,науковий ступінь,прізвище,ініціали) (підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

**Національний технічний університет України**
**«Київський політехнічний інститут імені Ігоря Сікорського»**

Факультет електроніки

Кафедра звукотехніки та реєстрації інформації

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (освітня програма) 171 «Електроніка» («Електронні системи мультимедіа та засоби Інтернету речей»)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Г.Г. Власюк
(підпис) (ініціали, прізвище)
« 26 » вересня 2018 р.

**ЗАВДАННЯ**
**на магістерську дисертацію студенту**

Наровському Олексію Михайловичу
(прізвище, ім'я, по батькові)

1 Тема роботи «Система забезпечення безпеки із застосуванням технології IoT»
керівник роботи Лазебний Володимир Семенович, к.т.н., доцент.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «07» листопада 2019р. №3859-с

2 Строк подання студентом дисертації 9 грудня 2019 р.
3. Об'єкт дослідження структура та технології систем забезпечення безпеки

4. Предмет дослідження (Вихідні дані – для магістерської дисертації за освітньо-професійною програмою) загальна оцінка загроз та вразливостей систем безпеки, які існують на сьогодні, та переспективних технологій, які можуть підвищити надійність системи

5. Перелік завдань, які потрібно розробити: проаналізувати види загроз в системах забезпечення безпеки, розглянути особливості технологій Інтернету речей для цих систем, дослідити захист інформації, запропонувати технології , що дозволять підвищити надійність і рівень безпеки в системах забезпечення безпеки

6. Перелік графічного (ілюстративного) матеріалу 9-12 слайдів презентації: формулювання завдання роботи, види загроз, порівняння технологій Інтернету речей, структура охоронної системи, захист інформації, висновки

7. Орієнтовний перелік публікацій:

1) Нові тенденції в СКУД / Наровський О. М. // III Всеукраїнська науково-технічна конференція «Сучасні технології кіно та аудіовізуальних систем - 2019»

8. Консультанти розділів дисертації

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |

9. Дата видачі завдання 26 вересня 2018 р.

Календарний план

| № з/п | Назва етапів виконання дипломної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Написання першого розділу | 17.03.2019 | |
| 2 | Написання другого розділу | 16.06.2019 | |
| 3 | Написання третього розділу | 12.10.2019 | |
| 4 | Написання четвертого розділу | 16.11.2019 | |
| | Написання п’ятого розділу | 26.11.2019 | |
| 5 | Підготовка матеріалів до друку та оформлення пояснювальної записки | 02.12.2019 | |
| 6 | Підготовка та оформлення презентації для доповіді | 08.12.2019 | |

Студент _____ О. М. Наровський
(підпис) (ініціали, прізвище)

Керівник роботи _____ В. С. Лазебний
(підпис) (ініціали, прізвище)

УДК 621.397.63

# РЕФЕРАТ

Магістерська дисертація: 103 с., 15 рис., 23 табл., 1 дод., 13 джерел

СИСТЕМИ БЕЗПЕКИ, ОХОРОННІ СИСТЕМИ, СКУД, БЕЗПРОВОДОВІ МЕРЕЖІ, WI-FI, BLUETOOTH, ZIGBEE, Z-WAVE, JEWELLER, ІНТЕРНЕТ РЕЧЕЙ, ПЕРЕДАВАННЯ ДАНИХ, БЕЗПЕКА, АВТЕНТИФІКАЦІЯ, ЗАХИСТ ІНФОРМАЦІЇ

**Актуальність роботи.** Сьогодні питання забезпечення безпеки є дуже важливим не тільки на підприємствах, фабриках, великих компаніях та державних установах, але й вдома. В такому випадку особливо важливу роль починають відгравати об’єднані охоронні системи, системи відеоспостереження, системи контролю і управління доступом, які завдяки технологічному прогресу почали переходити на більш сучасні рішення. І технології Інтернету речей їм в цьому допомагають.

Основною проблемою є відсутність повного захисту цих систем від різних загроз та факторів, як на апаратному так і на програмному рівні, що може призводити до втрати майна, цінної інформації або небажаних витрат.

**Мета і завдання дослідження.** *Метою* роботи є підвищення рівня надійності систем забезпечення безпеки, а саме охоронних систем, систем контролю та управління доступом, для запобігання небажаних наслідків від різних загроз та наявних вразливих місць.

Для досягнення поставленої мети необхідно вирішити такі *завдання*:

– проаналізувати види загроз в охоронних системах і системах контролю та управління доступом;

– дослідити підходи та вимоги до створення систем безпеки;

– розглянути особливості технологій Інтернету речей для охоронних систем та обмеження доступу;

– визначити організаційні засади та структуру різних систем забезпечення безпеки;

– дослідити захист в системах Інтернету речей та запропонувати технології, що дозволяють підвищити надійність і рівень безпеки в охоронних системах та системах управління та контролю доступом.

**Об'єкт дослідження** – структура та технології систем забезпечення безпеки.

**Предмет дослідження** – загальна оцінка загроз та вразливостей систем безпеки, які існують на сьогодні, та перспективних технологій, які можуть підвищити надійність системи.

**Методи дослідження** – теоретичне дослідження структури систем безпеки та основних вразливих місць, порівняльний аналіз різних технологій, які використовуються та можуть бути запропоновані для використання.

**Результат дослідження.** Запропоновано поєднання технологій передавання та захисту інформації для підвищення надійності системи та якісного покращення рівня безпеки, гнучкості в системах забезпечення безпеки.

**Апробація результатів дисертації.** Результати досліджень, що включені до дисертації, оприлюднені на III Всеукраїнській науково-технічній конференції «Сучасні технології кіно- та аудіовізуальних систем» (2019).

**Публікації**. Результати досліджень, наведених в дисертації, оприлюднено в таких виданнях:

1. О. М. Наровський. Нові тенденції в СКУД / П.В. Попович, О.М. Наровський// Матеріали конференції «Проектування та оптимізація інформаційних та телекомунікаційних систем». – К: КПІ ім. Ігоря Сікорського, 2019. - С. 19.

## SUMMARY

Today, the issue of security is very important not only in enterprises, factories, large companies and government agencies, but also at home. In this case, integrated security, video surveillance, access control and access control systems, which have begun to move to more advanced solutions, play a particularly important role. And the Internet of Things technology is helping them.

The subject of the study is a general assessment of the threats and vulnerabilities of security systems that exist today and of promising technologies that can improve system reliability.

The result of the work is the proposal to combine information transfer and security technologies to improve system reliability and quality improvement in security, and flexibility in security systems.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

AES – Advanced Encryption Standard;
API – Application Programming Interface;
BLE – Bluetooth Low Energy;
DNS – Domain Name System;
EID – Electronic Identification;
FTP – File Transfer Protocol;
IEEE – Institute of Electrical and Electronics Engineers;
IoT – Internet of Things;
IP – Internet Protocol;
MAC – Medium Access Control;
OCSP – Online Certificate Status Protocol;
OSDP – Open Supervised Device Protocol;
PoE – Power over Ethernet;
SAE – Simultaneous Authentication of Equals;
SCEP – Simple Certificate Enrollment Protocol;
SSID – Service Set Identifier;
TLS – Transport Layer Security;
WLAN – Wireless Local Area Network;
WMAN – Wireless Metropolitan Area Network;
WPA – Wireless Protected Access;
WPAN – Wireless Personal Area Network;
WWAN – Wireless Wide Area Network;

# ВСТУП

Як би нас не захоплювали окремі функціональні можливості пристроїв Інтернету речей, їх взаємодію для вирішення конкретних завдань представляється набагато більш важливим в сфері забезпечення безпеки. По-перше, системи на базі Інтернету речей повинні відрізнятися простотою в проектуванні, установці, обслуговуванні і експлуатації.

Це особливо відноситься до охоронних систем, функції яких поступово виходять далеко за межі спочатку закладених в камери відеоспостереження. Справді, саме завдяки Інтернету речей традиційні межі сфери відповідальності охоронних систем в наш час розширюються.

Інтернет речей поступово об'єднує в єдині системи такі раніше розрізнені пристрої, як камери відеоспостереження, детектори диму, датчики витоку газу, пристрої контролю фізичного доступу і гучномовці, дозволяючи створювати спільні диспетчерські для управління, контролю і спостереження за цілими комплексами будівель або ділянок різного призначення.

В результаті спочатку цільові охоронні системи набувають найширші можливості ділитися корисними даними з іншими підключеними пристроями з єдиним дистанційним управлінням.

Впровадження Інтернету речей відбувається не в глобальних масштабах, а всередині компаній. Складність впровадження полягає в тому, що жоден виробник не має в своєму складі закінченого рішення, що включає всі компоненти. Необхідно використання великої кількості систем від різних виробників і від їх правильного підбору та інтеграції залежить те, наскільки точно реалізоване рішення буде відповідати завданням і вимогам конкурентного середовища.

# 1 АНАЛІЗ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТЛОВИХ ТА ОФІСНИХ ПРИМІЩЕНЬ

Охорона власного майна здавна входить до списку основних факторів нашої цивілізації. З тих пір, як людина перестала вести кочовий спосіб життя, у неї відразу виникла потреба в захисті вмісту свого будинку. Разом з цим довелося вигадувати різні способи для запобігання появи чужих на своїй території. Першим логічним і досить ефективним методом був винахід дверей з різними засувами. Цей момент і став основоположним у довгому шляху розвитку технологій від простих замків до сучасних систем контролю і управління доступом та охоронних систем.

За останні 2 століття люди винайшли більше нововведень у всіх сферах, ніж за всю свою історію. Пов'язано це насамперед активним розвитком індустріальної епохи кінця 19 і початку 20 століть. Інженери навчилися працювати і синтезувати нові матеріали і сплави металів, в свою чергу розробки в електронних технологіях дозволили створити надмініатюрні компоненти. І тепер контроль доступу та охорону забезпечують абсолютно нові і розумні пристрої, які не знають слабкостей і працюють без будь-яких проблем.

## 1.1 Види загроз

Безпека організації, компанії, офісу, виробничого чи іншого приміщення забезпечується цілим комплексом заходів. До важливої складової виявлення загроз і їх нейтралізації відносяться системи безпеки. Системи безпеки забезпечують стабільність роботи організації, виконуючи різні функції захисту і контролю.

Аналізуючи систему безпеки потрібно розглянути види загроз, заради яких вона створюється, а також розглянути ті загрози, які можуть впливати на саму систему. Саме системи безпеки здатні впоратися з попередженням загроз, забезпечуючи контроль доступу на територію підприємства і об'єкти, що охороняються, моніторинг ситуації в режимі реального часу і прийняття термінових заходів у разі виникнення надзвичайних ситуацій.

Основні види загроз для офісних та житлових приміщень:

- спроба розкрадання майна або комерційної таємниці;
- підрив ділової репутації компанії;
- перехоплення управління;
- матеріальна шкода;
- виникнення пожежі, аварії та інших небезпечних для життя і здоров'я людей ситуацій.

Також потрібно врахувати інформаційну безпеку. Єдиної і загальноприйнятої класифікації загроз безпеки поки не існує. Однак можна класифікувати ці загрози з різних аспектів їх реалізації, способу їх здійснення і об'єкту атаки.

Класифікація загроз по цілі:

- несанкціоноване читання інформації;
- несанкціонована зміна інформації;
- несанкціоноване знищення інформації;
- повне або часткове руйнування операційної системи (під руйнуванням операційної системи розуміється цілий комплекс руйнівних впливів від короткочасного виведення з ладу окремих програмних модулів системи до фізичного стирання з диска системних файлів).

Класифікація загроз за принципом:

- використання відомих (легальних) каналів отримання інформації, (наприклад, загроза несанкціонованого читання файлу, доступ користувачів до якого визначено некоректно - дозволений доступ користувачеві, якому відповідно до адекватної політики безпеки доступ повинен бути заборонений);
- використання прихованих каналів отримання інформації(наприклад, використання зловмисником недокументованих всіх можливостей операційної системи);
- створення нових каналів отримання інформації з допомогу програмних закладок.

Класифікація загроз за характером впливу:

- активний вплив - несанкціоновані дії зловмисника в системі;
- пасивний вплив - несанкціоноване спостереження зловмисника за процесами, що відбуваються в системі.

Класифікація загроз на кшталт використовуваної зловмисником слабкості захисту:

- неадекватна політика безпеки, в тому числі і помилки адміністратора системи;
- помилки і недокументовані можливості програмного забезпечення операційної системи, в тому числі і так звані люки;
- випадково або навмисно вбудовані в систему "службові входи", що дозволяють обходити систему захисту(зазвичай люки створюються розробниками програмного забезпечення для тестування і налагодження, і іноді розробники забувають їх видалити або залишають спеціально);
- раніше впроваджена програмна закладка.

Класифікація загроз за способом впливу на об'єкт атаки:

- безпосередній вплив;
- перевищення користувачем своїх повноважень;
- робота від імені іншого користувача;
- використання результатів роботи іншого користувача (наприклад, несанкціоноване перехоплення інформаційних потоків, ініційованих іншим користувачем).

Класифікація загроз за способом дій зловмисника (порушника):

- в інтерактивному режимі (вручну);
- в пакетному режимі (за допомогою спеціально написаної програми, яка виконує негативні впливи на операційну систему без безпосередньої участі користувача-порушника).

Класифікація загроз по об'єкту атаки:

- операційна система в цілому;
- об'єкти операційної системи (файли, пристрої тощо);

- суб'єкти операційної системи (користувачі, системні процеси, тощо);
- канали передачі даних.

Класифікація загроз по використовуваних засобах атаки:

- штатні засоби операційної системи без використання додаткового програмного забезпечення;
- програмне забезпечення третіх фірм (до цього класу програмного забезпечення відносяться як комп'ютерні віруси та інші шкідливі програми, які можна легко знайти в інтернеті, так і програмне забезпечення, спочатку розроблене для інших цілей: мережеві монітори, сканери, тощо.);
- спеціально розроблене програмне забезпечення.

Класифікація загроз за станом об'єкта, що атакується операційної системи на момент атаки:

- зберігання;
- передача;
- обробка.

Класифікація загроз за силою впливу на область ураження виділяються:

- руйнівні;
- дестабілізуючі;
- паралізуючі;
- стимулюючі загрози;

Класифікація фізичних загроз:

- знищення або руйнування засобів обробки інформації і зв'язку;
- розкрадання носіїв інформації;
- розкрадання програмних або апаратних ключів і засобів криптографічного захисту даних;
- вплив на персонал;

Класифікація радіоелектронних загроз:

- впровадження електронних пристроїв перехоплення інформації в технічні засоби і приміщення;

- перехоплення, дешифрування, підміна і знищення інформації в каналах зв'язку[1].

### 1.2 Підходи та вимоги до створення систем безпеки

Сучасний стан проблеми забезпечення безпеки визначається безліччю факторів. Найбільш суттєвими з них є ті, які безпосередньо формують основні оцінки ситуації, принципи діяльності всіх структур у сфері забезпечення безпеки.

Аналіз певного обсягу аналітичного матеріалу дозволяє зробити деякі висновки про тенденції, що складаються при створенні, модернізації систем забезпечення безпеки. На даний момент у фахівців служби безпеки є зацікавленість і готовність до практичних кроків в застосуванні ефективних систем, а саме:

- визнання необхідності у використанні нових елементів в структурі системи;
- розуміння необхідності етапу проектування в побудові системи, як елементу технології;
- оптимізації структури і функціональних характеристик комплексу.

Обґрунтування і оптимізація структури і функціональних характеристик системи, розробка вимог і рекомендацій до її елементів є основним змістом і метою діяльності в сфері створення та функціонування систем забезпечення безпеки. Ця робота включає в себе:

- категоріювання об'єкта;
- вибір критерію ефективності створюваної або модернізованої системи;
- проведення аналізу вразливості об'єкта для оцінки ефективності існуючої та створюваної системи;
- формування вимог до складу та функціональних характеристик системи;
- розробку концептуального рішення щодо створення, модернізації системи;
- вибір і оптимізацію структури системи;
- внесення змін до концепції створення системи при зміні загроз і умов функціонування об'єкта.

Категоріювання проводиться з метою визначення ступеня небезпеки об'єкта в умовах гіпотетичної реалізації встановлених видів загроз і вирішується експертними методами шляхом визначення видів і масштабів збитку, який може виникнути в разі реалізації загроз. Результатом є віднесення об'єкта до відповідної категорії, що, в свою чергу, визначає загальні вимоги до системи забезпечення безпеки і дозволяє задати кількісні критерії ефективності системи, необхідні в подальшому для її оцінки.

Наступним кроком має бути визначення ступеня відповідності існуючої системи забезпечення безпеки вимогам, пред'явленим в результаті категоріювання. Для цього необхідне проведення аналізу вразливості об'єкта. Створення, модернізація систем забезпечення безпеки без аналізу ситуації на об'єкті захисту, аналізу вразливості об'єкта і науково обґрунтованих рекомендацій може призвести, наприклад, до того, що не будуть враховані якісь важливі загрози, а в створення, модернізацію системи безпеки будуть вкладені кошти, що перевищують реально необхідні.

Аналіз вразливості об'єкта виконується експертними методами та (або) методами імітаційного моделювання і включає в себе:

- комплексну оцінку ефективності існуючої системи забезпечення безпеки, при встановлених видах загроз і пріоритетах цілей захисту, шляхом порівняння отриманих розрахункових даних з заданими критеріями;
- розробку заходів по досягненню заданих критеріїв;
- оцінку, підтвердження ефективності цих заходів.

Заходи по досягненню заданих критеріїв ефективності є, по суті, вимогами до структури і функціональних характеристик системи забезпечення безпеки, що створюється або модернізується і тим самим завершують етап розробки концепції створення системи. Результатами цього етапу є:

- рекомендації щодо структури та змісту організаційно-розпорядчих документів про забезпечення безпеки об'єкта;
- проект організаційно-штатної структури та рекомендації щодо організації сил охорони об'єкта;

- вимоги за призначенням до інженерно-технічних засобів і систем, що входять в систему забезпечення безпеки (ці вимоги є основою для розробки технічного завдання на її проектування);

Аналіз повинен проводитися із залученням спеціалізованих організацій, що мають у своєму складі кваліфікованих фахівців в різних областях знань і мають спеціальне програмно-методичне забезпечення.

Тільки при такому підході можна забезпечити об'єктивність і високу якість аналізу вразливості і створити ефективну систему забезпечення безпеки, економічно доцільну для об'єкта захисту. Провідними фірмами в даний час пропонуються різні варіанти побудови систем. Тому завдання оптимізації вибору системи, яка найкращим чином відповідає вимогам конкретного об'єкта, також стало елементом науково-методичного супроводу створення системи забезпечення безпеки. Існуючі підходи до вирішення задачі оптимізації структури системи використовують різні методики і при достатній кваліфікації аналітиків і експертів дозволяють отримувати адекватні результати.

Таким чином, науково-методичний супровід створення системи дозволяє забезпечити:

- адекватність системи встановленим загрозам;
- здатність системи гнучко реагувати на зміни загроз і умов функціонування об'єктів захисту;
- оптимальну побудову системи за критерієм «ефективність-вартість»;
- оптимізацію структури системи забезпечення безпеки в цілому.

А науково-методичний супровід, що проводиться з метою обґрунтування і розробки основних вимог до систем забезпечення безпеки потенційно небезпечних об'єктів, є обов'язковим етапом робіт зі створення систем.

Проте все ж можна виділити основні технічні вимоги до систем, що проектуються. Вони включають в себе:

- основні функціональні вимоги до підсистем;
- вимоги по стійкості до зовнішніх чинників;
- вимоги щодо електромагнітної сумісності;

- вимоги щодо електробезпеки;
- вимоги з електропостачання.

Крім того, повинен бути при необхідності обговорений порядок організації випробувань, приймання комплексу в експлуатацію, порядок організації дослідної експлуатації, порядок проведення технагляду.

Для забезпечення повної безпеки в організаціях встановлюються системи контролю доступу та сканери безпеки, системи сигналізації та відеоспостереження, системи протипожежного захисту, а також застосовуються інші методи.

Охоронна система та  система контролю і управління доступом забезпечує безпеку вашої оселі або офісу, підприємства, тощо, як від зовнішнього проникнення, так і від аварій всередині приміщення. До всіх вікон та дверей підключаються датчики відкриття. У кімнатах встановлюються датчики руху та відеокамери. При бажанні, ви з будь-якої точки світу, завжди будете бачити, що відбувається у вашому домі чи офісі. Це важливо, як при захисті будинку від сторонніх, так і в разі, якщо ви залишаєте дітей вдома з нянею. Окремо, в будинку, встановлюються датчики витоку газу та протікання води. При спрацьовуванні вони перекривають захисні клапани, завдяки цьому ваш будинок залишається цілим та неушкодженим.

Встановивши камери відеоспостереження, ви завжди можете контролювати ситуацію в вашому домі. При цьому, камери можуть виконувати не тільки охоронну функцію. Як було вказано вище, ви можете простежити за тим, як доглядає за близькою людиною доглядальниця або як займається з дитиною няня.

**Висновки до розділу**

1. Проектуючи систему забезпечення, безпеки потрібно розглядати види загроз, заради яких вона створюється, а також розглядати ті загрози, які можуть впливати на саму систему.

2. Аналізуючи підходи та вимоги до створення систем безпеки, потрібно враховувати, для чого саме вона створюється та де буде застосовуватись, за яких

умов та обставин. Виходячи з цих даних, можна розглядати різні можливості системи.

3. Для досягнення мети дисертаційного дослідження необхідно:

- дослідити технології Інтернету речей для охоронних системи та систем обмеження доступу;
- розглянути організаційні засади та структуру різних систем забезпечення безпеки;
- дослідити захист інформації в системах Інтернету речей.

# 2 ДОСЛІЖЕННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ОХОРОННИХ СИСТЕМ ТА СИСТЕМ ОБМЕЖЕННЯ ДОСТУПУ

Інтернет речей описує дуже важливий етап розвитку глобальної мережі, що характеризується підключенням великої кількості пристроїв, які здійснюють автоматизовану обробку даних без участі людини.

Основним призначенням мережі інтернет є здійснення транспортної функції: об'єднання приватних обчислювальних мереж, індивідуальних користувачів і центрів обробки даних. Фізичний рівень глобальної мережі досить статичний і вдосконалюється в основному в кількісному відношенні шляхом підвищення пропускної здатності каналів зв'язку і обладнання, яке створює канали.

Значне збільшення трафіку призводить до розробки все більш потужних маршрутизаторів і вдосконалення протоколів маршрутизації і принципів функціонування мережі. У побудові сучасних мереж, крім традиційного інфраструктурного рівня передачі даних, що містить обладнання для маршрутизації та комутації, виділяється рівень управління.

Поділ функцій передачі та управління дозволяє віртуалізувати мережеву інфраструктуру і значно підвищити утилізацію і централізувати управління ресурсами, реалізуючи технологію програмно-визначених мереж, призначену для роботи в умовах динамічних змін.

Такий підхід вже сьогодні знаходить своє застосування в центрах обробки даних при побудові хмарних сервісів і стрімко набирає популярність в корпоративних мережах і мережах провайдерів.

Цінністю мережі інтернет є ряд спеціалізованих сервісів, реалізованих на її базі – DNS, електронної пошти (e-mail), передачі файлів (FTP), всесвітньої павутини (World Wide Web), потокового мультимедіа тощо. Надані сервіси знаходяться в безперервному розвитку, трансформуючи суспільство в рамках мережі. Більшість додатків використовує модель взаємодії «користувач - сервіс» і є відображенням формованого інформаційного суспільства.

Важливим етапом розвитку мережі інтернет є поява концепції хмарних

обчислень. В основу концепції покладено принцип загального використання програмно-апаратної інфраструктури провайдера. Такий підхід дозволяє користувачам зменшувати витрати і при необхідності гнучко нарощувати інформаційні ресурси.

Цифрові технології стають все доступнішими і є основним елементом підвищення продуктивності праці, впровадження інновацій та підвищення якості життя.

Все більше найрізноманітніших пристроїв, що використовують технологію міжмашинної взаємодії «M2M, machine to machine», підключаються до мережі інтернет. В рамках такого технологічного рішення використовується ряд спеціалізованих пристроїв, які збирають інформацію телеметричного характеру.

Ключовою властивістю таких систем є їх індустріальна спрямованість і необхідність участі людини в прийнятті управлінських рішень. Саме цей аспект сильно обмежує застосування M2M-технологій і привів до вдосконалення концепції і появи поняття «Інтернет речей».

Інтернет речей є мережею різноманітних підключених до інтернету пристроїв, що реалізують різні моделі взаємодії - «Річ - Річ» (Thing-Thing), «Річ - Користувач» (Thing-User) і «Річ - Веб-Об'єкт» (Thing-Web Object). З'єднання «розумних речей» в єдину мережу надає критично важливі якісні зміни для розвитку людської життєдіяльності. Однією з головних передумов до цього є перехід до використання в мережі інтернет-протоколу IPv6, що дає можливість надати виділену унікальну адресу кожному пристрою, що підключається. При цьому основну частину з об'єктів, що підключаються, будуть складати різноманітні спеціалізовані пристрої, що мають в своєму складі мікроконтролер з різними платами розширення - модуль передачі даних, модуль пам'яті, засоби вимірювання і засоби ідентифікації. Для управління пристроєм, обробки і передачі даних на контролері використовується операційна система реального часу, що відповідає за збір і первинну обробку даних для мінімізації трафіку.

Поширення розумних речей робить нераціональним використання традиційної моделі «Клієнт - Сервер» з точки зору обміну трафіком. У місцях їх

знаходження часто дуже важко забезпечити високошвидкісні канали з низькою затримкою, а власна обчислювальна потужність дозволяє проводити необхідну обробку даних, реалізуючи концепцію «туманних обчислень». Функціональним елементом туманних обчислень є мікроконтролери, які об'єднуються в розподілену обчислювальну мережу. Їх завдання здійснювати зберігання та обробку інформації, що надходить, надаючи обчислювальні потужності для різноманітних прикладних задач, які здійснюють адміністрування систем без участі людини. Отримувані ж на цьому рівні структуровані дані можуть передаватися через спеціалізовані інтерфейси програмування додатків (API – Application Programming Interface) в різноманітні системи хмарних обчислень для подальшої обробки, в тому числі і з залученням людських ресурсів.

Як канали зв'язку використовуються конвергентні мережі на базі протоколу IP, а місця установки датчиків настільки різноманітні, що використання проводової інфраструктури дуже обмежено. Їх підключення все частіше здійснюється за допомогою безпроводових технологій. До недавнього часу для цього використовувалися традиційні технології для користувальницької передачі даних – Wi-Fi, 2G, 3G.

Мультисервісна мережа дозволяє підключати пристрої телеметрії для спостереження за станом виробничих об'єктів в режимі реального часу. Характерною особливістю такого проекту є наявність електроживлення на кожному об'єкті, що підключається, але, на жаль, так буває не завжди. І проблема забезпечення електроживлення датчиків стоїть дуже гостро, ускладнюючи застосування радіотехнологій.

Зараз в технології міжмашинної взаємодії для зв'язку все ще застосовують ієрархії протоколів, розроблені IEEE (Institute of Electrical and Electronics Engineers). Відповідно до її принципів всі безпроводові мережі сьогодні прийнято ділити на чотири типи: персональні WPAN (Wireless Personal Area Network), локальні WLAN (Wireless Local Area Network), міські WMAN (Wireless Metropolitan Area Network) і глобальні WWAN (Wireless Wide Area Network) безпроводові мережі.

Складнощі з організацією електроживлення знижують популярність мереж

сімейства стандартів 802.11. Для підключення розумних пристроїв на невеликих відстанях (до 10 метрів) застосовуються стандарти, що використовують mesh-архітектуру, що володіють підвищеною живучістю і розроблені для мінімізації енергоспоживання, – 6LoWPAN, Bluetooth Low Energy (BLE), ZigBee, Z-Wave, EnOcean і тощо. А для організації зв'язності на великих відстанях розробляється ряд спеціалізованих радіотехнологій з низьким енергоспоживанням.

На вертикальних ринках вже використовується ряд технологій - C-UNB (Cooperative Ultra Narrowband), LoRa (Long Range), але найперспективнішими для Інтернету речей є технології EC-GSM (Extended Coverage GSM) і NB-CIoT (Narrowband Cellular IoT), які передбачають використання мереж мобільного зв'язку. Для цієї мети планується виділяти смуги частот нижче використовуваних в мобільних мережах, і операторам необхідно тільки додати відповідні трансивери на базових станціях і оновити ПЗ.

З'єднання розумних об'єктів в єдину мережу за допомогою IP-протоколу утворює мережу мереж, продукує велику кількість найрізноманітніших телеметричних даних. І цінність одержуваної інформації цілком визначається протоколами прикладного рівня, що працюють поверх мережі.

Головним завданням при цьому є однозначна ідентифікація кожного елемента. З огляду на необхідну розрядність краще всього для цього підходить унікальна IPv6 адреса, що виділяється кожному пристрою в сучасних мережах. Ідентифікатор використовується не тільки для маршрутизації пакетів, але і для зіставлення з фізичними параметрами властивими пристроїв (mac-адреса, RFID, Electronic Identification (EID), QR-кодами тощо).

Розумні об'єкти, що володіють унікальним ідентифікатором, в залежності від конструкції, здатні не тільки передавати потоки даних, що збираються сенсорами, а й здійснювати передачу команд для зміни стану підключених до них пристроїв.

Протоколи взаємодії між цими компонентами є стеком стандартів, які добре себе зарекомендували, адаптованих для використання через низькошвидкісні канали. Обмін повідомленнями працює за схемою видай/підпишись (Publish/subscribe). Для цього виділяється спеціалізований «сервер» для передачі

інформації – брокер. Вся передана інформація поділяється за напрямками на різні канали. Різноманітні датчики передають інформацію про різні фізичні величини по відповідних каналах, в той час як споживачі підписуються на їх отримання, дуже гнучко обмінюючись необхідною інформацією. Описаний принцип набув широкого поширення в цілому ряді протоколів – MQTT (MQ Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol, AMQP (Advanced Message Queuing Protocol) і тощо.

Найбільш цікавим є протокол CoAP (Constrained Application Protocol). Він є адаптацією протоколу Web (web transfer protocol) для роботи за технологією міжмашинної взаємодії. Він не тільки добре інтегрується з HTTP, а й підтримує адміністрування підключених пристроїв.

Система управління відповідає за конфігурацію, оновлення програмного забезпечення та моніторинг роботи обладнання. Можливості управління розумними об'єктами істотно менше в порівнянні з класичними пристроями (маршрутизаторами, комп'ютерами, серверами тощо) і мають свою специфіку. Для цих цілей розроблено ряд стандартів, які працюють за технологією Клієнт – Сервер: CWMP, OMA-DM, Lightweight M2M тощо.

Все частіше ми чуємо про злом пристроїв і їх використанні в шкідливих цілях, а всі питання безпеки вирішуються індивідуально кожним виробником пристроїв і програмного забезпечення. З огляду на широту поширення розумних об'єктів і ускладнення цільових атак, не дивно, що посилена увага в розробці протоколів приділяється безпеці.

Заходи щодо забезпечення безпеки можна умовно розділити за чотирма напрямками – підключення, ідентифікація, шифрування трафіку і безпеку додатків.

Збереження цілісності та конфіденційності даних досягається застосуванням шифрування для автентифікації і збереження цілісності повідомлень. Процедура передбачає підтвердження даних користувача і ліквідності використовуваних сертифікатів, що досить складно реалізувати в глобальних масштабах, тому виробники часто жорстко вбудовують облікові дані в програмно-апаратний комплекс. Ця інформація дозволяє чітко ідентифікувати пристрій, але не годиться

для забезпечення цілісності даних. На транспортному рівні питання безпеки передачі даних вирішується в рамках протоколів Transport Layer Security (TLS) і Datagram TLS (DTLS) шляхом створення захищеного тунелю для додатків.

Але незважаючи на це, додатки є самою вразливою частиною рішення. Їх безконтрольне поширення становить серйозну загрозу. Надання розподіленої платформи для обробки даних різними додатками – одна з особливостей архітектури Інтернету речей, і основні тенденції в удосконаленні протоколу їх безпечного підключення це виявлення розумних речей і їх автентифікація, використання цифрових ідентифікаторів і централізоване управління доступом до ресурсів. І майбутнє глобальних туманних обчислень цілком залежить від можливості взяти процеси під контроль і забезпечити безпечну розподілену інформаційну мережу, яка самостійно конфігурується.

Впровадження Інтернету речей відбуваються не в глобальних масштабах, а всередині компаній. Технологія розумних речей здатна підвищити продуктивність праці в першу чергу у виробничому сегменті, логістичному бізнесі, транспортних і енергетичних компаніях. Складність впровадження полягає в тому, що жоден виробник не має в своєму складі закінченого рішення, що включає всі компоненти. Необхідно використання великої кількості систем від різних виробників і від їх правильного підбору та інтеграції залежить те, наскільки точно реалізоване рішення буде відповідати завданням і вимогам конкурентного середовища.

Якщо ми складемо рейтинг основних тенденцій розвитку технологій, очолять його саме мережеві системи. Тому що можливості систем на базі IP-технологій безперервно розширюються, а постачальники всіх видів обладнання постійно шукають і знаходять все нові шляхи нарощування потужності, гнучкості і радіусу дії мережевих систем. У міру того, як охоронні пристрої на базі IP-технологій неухильно йдуть на зміну застарівшим аналоговим системам, розширюється і застосування охоронної апаратури, яке об'єднує потоки інформації в середовищі Інтернету речей вже не тільки в інтересах безпеки, але і для вирішення безлічі інших завдань в найрізноманітніших сферах.

Як би нас ні захоплювали окремі функціональні можливості пристроїв

Інтернету речей, їх взаємодію для вирішення конкретних завдань представляється набагато більш важливим в сфері забезпечення безпеки. По-перше, системи на базі Інтернету речей повинні відрізнятися простотою в проектуванні, установці, обслуговуванні і експлуатації. Щоб скористатися потенціалом Інтернету речей в повній мірі, постачальникам систем потрібно глибоке знання предмета, а також:

- розуміння принципів взаємодії всіх функцій та компонентів;
- вміння розроблювати системи під конкретні завдання;
- здатність реалізовувати такі комплексні рішення, які приносили б довготривалу користь, яка в сумі перевищує ефект від сукупності окремих компонентів.

Це особливо відноситься до охоронних систем, функції яких поступово виходять далеко за межі спочатку закладених в камери відеоспостереження. Справді, саме завдяки Інтернету речей традиційні межі сфери відповідальності охоронних систем в наш час неухильно розмиваються. Так, наприклад, мережеві камери все ширше застосовуються в інформаційних системах обслуговування будівель і споруд , в бізнес-аналітиці, в сфері роздрібної торгівлі, навіть в наукових дослідженнях і аналізі схем руху транспорту і потоків людей в реальному часі. Інтернет речей поступово об'єднує в єдині системи такі раніше розрізнені пристрої, як камери відеоспостереження, детектори диму, датчики витоку газу, пристрої контролю фізичного доступу і гучномовці, дозволяючи створювати спільні диспетчерські для управління, контролю і спостереження за цілими комплексами будівель або ділянок різного призначення.

В результаті спочатку цільові охоронні системи набувають найширші можливості ділитися корисними даними з іншими підключеними пристроями з єдиним дистанційним управлінням.

Потоки даних, які постійно зростають, із загальним доступом до них через мережу, а часто і з можливістю їх зберігання і обробки в «хмарі», створюють зростаючий попит на засоби захисту цих даних і інших «віртуальних» ресурсів, тобто на нові технології і способи підвищення кібербезпеки для захисту мережевих і «хмарних» охоронних систем. Таким чином, усунення вразливостей і захист від

спроб мережевого злому стає критично важливим аспектом проектування і впровадження систем фізичної безпеки і охоронного відеоспостереження.

Стрімке проникнення «хмарного» обчислювального середовища практично в усі галузі не обійшло стороною і індустрію безпеки разом з охоронним відеоспостереженням. Послуги із забезпечення безпеки з дистанційним управлінням вивільняють цінні людські та фінансові ресурси, бо присутність людей на кожному об'єкті, який знаходиться під наглядом, вже не потрібно. Розширюється застосування віддаленого доступу до охоронних систем, надзвичайний зручне тим користувачам, яким потрібно організувати спостереження за майном і подіями в реальному часі без фізичної присутності.

«Хмарні» сховища даних служать ще одним прикладом підвищення ефективності систем, розроблених на основі цієї моделі. Засоби економічного, надійного зберігання даних в обсягах, що багаторазово перевищують можливості виділених серверних систем, дозволяють архівувати відеозаписи та відповідні відомості на більш тривалі терміни, спрощуючи до них доступ.

Безпроводові технології перевернули наше життя безліччю способів: від мобільних телефонів до мереж Wi-Fi. Вже зараз ми широко користуємося перевагами і зручністю дистанційного охоронного відеоспостереження через смартфони і планшети. Програмним забезпеченням систем охоронного відеоспостереження, які налічують до десятка мережевих камер, можна цілком і повністю керувати за допомогою мобільних пристроїв без необхідності в настільних ПК. Це істотно знижує психологічні бар'єри технічної властивості, особливо для малого та середнього бізнесу, де користувачі віддають перевагу програмам для смартфонів, в порівнянні з більш ґрунтовним і детальним комп'ютерним ПЗ для управління відеоспостереженням. Крім того, знижуються і загальні витрати на системи, включаючи їх обслуговування.

Ринок СКУД не стоїть на місці: з'являються нові способи ідентифікації, розвиваються традиційні рішення, контроль доступу все більше зближується з IT-інфраструктурою, дозволяючи створювати багатофункціональні комплексні системи і вирішувати найрізноманітніші проблеми користувачів. В умовах, що

склалися на ринку систем контролю і управління доступом конкуренція зростає, спонукаючи виробників удосконалювати свої продукти для найсучасніших запитів ринку.

Сучасні контролери СКУД відрізняються від попередників не тільки підвищеною продуктивністю, об'ємом пам'яті і іншими кількісними показниками, а й якісно новою логікою роботи, а також підвищеною захищеністю. Фактично такі контролери можна назвати спеціалізованими комп'ютерами, що мають на борту свою операційну систему, що дозволяє задавати різноманітні і складні сценарії роботи СКУД на апаратному рівні і адекватно реагувати на знову виникаючі загрози шляхом простої зміни прошивки інтегрованої програмної оболонки. Реалізація критичних функцій системи не тільки на програмному, а й на апаратному рівні істотно підвищує надійність. У цьому випадку навіть при втраті зв'язку з сервером система продовжить працювати, зберігаючи найбільш важливий функціонал.

Важливим трендом стало поширення серед контролерів СКУД захищеного OSDP-інтерфейсу (Open Supervised Device Protocol) між зчитувачем і контролером. Класичний Wiegand втрачає завойовані позиції. Протокол OSDP другого покоління з шифруванням за алгоритмом AES-128 забезпечує передачу даних між пристроями в захищеному вигляді. Даний протокол дозволяє користувачеві отримати важливий зворотній зв'язок від зчитувача, своєчасно виявляти його відключення або несправність. Також цікаво відзначити інше: як OSDP пристрої, що підключаються до контролерів СКУД, можуть виступати не тільки зчитувачі, це можуть бути релейні модулі, кнопки виходу, електрозамки і інша периферія. Все це виводить контролери СКУД на новий рівень функціональності, причому стандартизація інтерфейсу дозволяє використовувати модулі різних виробників[2].

Також хотілося б зазначити, що в майбутньому технологія доступу по смартфону буде рівноцінна використанню карт. Застосування смартфонів зручно для користувача і підвищує рівень безпеки системи. Але смартфон в більшості випадків є приватною власністю, і потрібно отримати у власника (працівника) дозвіл на установку програмного додатка. У той же час адміністратор карткової СКУД може завжди забрати карту людини, яка звільнилася і передати її новому

співробітнику без покупки нового ідентифікатора. Крім того, телефон може просто розрядитися, і ідентифікатор стане недоступний. З огляду на ці нюанси, можна сказати, що, звичайно, зручно проходити по телефону, але в ряді випадків карта залишиться актуальною ще довгий час[3].

Говорячи про Інтернет речей, для повноцінного функціонування такої мережі необхідна автономність всіх «речей», тобто датчики повинні навчитися отримувати енергію з навколишнього середовища. Проте розглянемо різні технології, які допомагають реалізувати Інтернет речей в охоронних системах та системах обмеження доступу, адже саме завдяки Інтернету речей з'явилося багато мов і протоколів[7].

Область 2,4 ГГц використовується в усьому світі для Wi-Fi і інших протоколів персональних локальних мереж. Застосовувані в цій області частот стандарти безпроводового зв'язку (Bluetooth, ZigBee, Wi-Fi, тощо) користуються популярністю в багатьох сферах уже протягом кількох років. Реалізація таких рішень легко доступна, оскільки для цього є велика кількість мікросхем і повністю закінчених модулів, які можна без особливих зусиль інтегрувати і використовувати при розробці IoT-пристрою. Якщо вибрати проектування на рівні чіпу, то це забезпечить більшу гнучкість, оскільки можна буде застосувати нові інтегральні схеми з розширеними функціями і більш високою продуктивністю або ті, які необхідні саме для IoT-пристрою. Але тоді всі питання, включаючи тестування на відповідність стандартам, доведеться вирішувати самостійно.

Що стосується радіочастотних модулів, то це невеликі плати, на яких мікросхеми, контролери, програмне забезпечення (ПЗ) і навіть антена вже протестовані і сертифіковані на відповідність необхідним стандартам і заданим в специфікації характеристикам. Відповідність вимогам заздалегідь забезпечує виробник модуля. Завдяки цьому дотримання стандартів в частині радіоканалів при випробуваннях кінцевого обладнання значно полегшується. Такий підхід також дозволить скоротити час розробки проекту і зменшити або навіть повністю виключити витрати часу на перевірку відповідності. Однак все це досягається за рахунок більш високих витрат на компоненти, ніж при самостійному виконанні

індивідуальної конструкції на основі інтегральних радіочастотних мікросхем. Тому до питання вибору компонентів потрібен особливий підхід.

Більшість стандартів для безпроводових систем зв'язку ближнього радіусу дії відноситься до організації персональної мережі - тієї, яка побудована «навколо» людини. Така мережа в технічній літературі іноді скорочено іменується PAN (Personal Area Networks), хоча для нас більш звичні інші назви - наприклад, WLAN (Wireless Local Area Network). PAN - це мережа передачі даних, яка об'єднує персональні електронні пристрої одного користувача: телефони, кишенькові персональні комп'ютери, смартфони, ноутбуки, бездротові гарнітури тощо. Зазвичай такі мережі мають радіус покриття від 10 до 30 метрів.

Пристрої для організації персональної мережі ближнього радіусу дії іноді оптимізуються для певних програм за допомогою протоколів, званих «профілі додатків» (Application Profile) або використовують подібні ідентифікатори. Такі протоколи адаптуються під конкретні сфери: охорона здоров'я, спорт, засоби контролю і промислової автоматизації, моніторинг будівель і споруд тощо. Спеціальні профілі дозволяють пристроям реалізовувати підмножини всіх безпроводових стандартів IoT за рахунок оптимізації вбудованого ПО і складності самого пристрою, завдяки чому можна знизити загальні витрати і заощадити енергію акумулятора. Стандарти організації безпроводових мереж IoT постійно розвиваються, але подібні профілі можуть використовуватися і для нових версій стандартів, навіть якщо вони несумісні з більш ранніми специфікаціями.

Для простих радіочастотних ліній зв'язку «точка-точка» були розроблені специфікації більш високого рівня: протоколи для мережевих, транспортних і навіть прикладних рівнів. Тому ваш остаточний вибір безпроводових технологій, найімовірніше, буде включати рішення в частині ПЗ, пов'язані з поставленою кінцевою метою і областю використання даних конкретного IoT-пристрою.

Однак потрібно звернути увагу на важливий момент. До мільярдів вже діючих безпроводових пристроїв в найближчі кілька років приєднається ще кілька мільярдів, в зв'язку з чим багато-які смуги частот, які використовуються, стануть переповненими, а взаємний вплив пристроїв - ще більшою проблемою. У деяких

середовищах, наприклад, в лікарнях, нові безпроводові пристрої просто не в змозі нормально функціонувати через взаємні завади, які створюють випромінюючі радіочастоти пристрої, тому вибір смуги частотного спектру і виду модуляції для нового продукту повинен обов'язково враховувати цей фактор. Хоча деякі стандарти безпроводового зв'язку мають можливості виявлення і запобігання впливу зовнішніх завад, вони зазвичай роблять це в рамках своїх протоколів зв'язку і не розпізнають чужі. Тому технології з різними протоколами зв'язку в радіочастотному середовищі не є достатньо ефективними, особливо в тому випадку, коли кілька пристроїв, як уже було сказано вище, використовує одну загальну смугу частотного спектра[13].

## 2.1 Технологія Wi-Fi

Під абревіатурою Wi-Fi (від англійського словосполучення Wireless Fidelity, яке можна дослівно перекласти як «висока точність безпроводової передачі даних») в даний час розвивається багато стандартів передачі цифрових потоків даних по радіоканалах. Це сучасна безпроводова технологія з’єднання пристроїв в локальну мережу і підключення їх до Інтернету. Саме за допомогою цієї технології Інтернет стає мобільним і дає користувачеві свободу переміщення як в межах однієї кімнати, так і по всьому світу.

Принцип роботи технології Wi-Fi полягає в використанні радіохвиль частотою 2,4МГц і 5 МГц для передачі даних між адаптером і маршрутизатором в мережі. Використовуються 13 частотних каналів в 2,4 ГГц діапазоні і 4 частотних смуги в сумі з 23 каналами в 5 ГГц діапазоні. На сьогоднішній день існує безліч стандартів Wi-Fi, що відрізняються своїми технічними характеристиками: відстанню, швидкістю тощо. Найбільш популярними є стандарти 802.11b, g, n, ac. Стандарт 802.11a не отримав належного поширення в країнах Європи. Стандарти 802.11b, g працюють на частоті 2,4 ГГц зі швидкостями передачі даних 11 Мбіт/с і 54 Мбіт/с відповідно. 802.11n був затверджений в 2009 році і може працювати як на частоті 2,4 ГГц, так і 5 ГГц, використовуючи ортогональное частотне

мультиплексування сигналу, як і 802.11g. Максимальна швидкість передачі становить 600 Мбіт/с (4 приймаючих антени), 150 Мбіт/с (1 приймаюча антена). Стандарт 802.11ac використовує частоту 5 ГГц і дозволяє передавати дані зі швидкістю до 1,3 Гбіт/с.

Проте розглянемо як ця технологія показує себе в системах безпеки. Наприклад охоронні системи з Wi-Fi сигналізацією нового покоління, що використовують інноваційну технологію обміну даними через Інтернет між Wi-Fi сигналізацією і смартфонами користувачів. Перші системи Wi-Fi сигналізації вийшли на ринок охоронного обладнання відносно недавно, але завдяки розширеним можливостям і зручності в користуванні Wi-Fi сигналізація стала стрімко займати лідируючі позиції серед охоронного обладнання категорії для самостійного встановлення.

Звичайно, потрібно відразу визнати, що Wi-Fi сигналізація має як ряд переваг, так і деякі недоліки. Wi-Fi сигналізація працює через Інтернет і має безпроводовий Wi-Fi зв'язок тільки з нашим роутером, який в свою чергу в більшості випадків отримує зв'язок з Інтернетом по кабелю.

Як відомо, одним із стовпів, на яких тримається успіх Інтернету речей, є потреба підключити безліч IoT-пристроїв до решти світу через Інтернет. Можна з упевненістю припустити, що основою для цього стане саме безпроводовий зв'язок. Питання залишається в тому, яка з технологій буде найбільш вдалою. Зараз існує багато варіантів, кожен з яких пропонує різні способи встановлення з'єднання для додатків Інтернету речей. Найбільш популярними є Wi-Fi, Bluetooth і їх різновиди, а також LTE на базі стільникового зв'язку. Конкретний вибір буде залежати вже від певних області застосування, діапазону і смуги частот, пропускної здатності каналу передачі даних і часу автономної роботи. У якихось випадках, можливо, навіть буде необхідна комбінація технологій.

Технологія Wi-Fi не обмежується мережами малого радіусу і невеликою зоною покриття. З'являються постачальники, які надають обладнання для забезпечення безпроводового зв'язку на великих відстанях з використанням частот і типів модуляції технології Wi-Fi в поєднанні з більш великими і ефективними

антенами, в деяких випадках вузьконаправленими. Крім того, в такому обладнанні, як правило, застосовується технологія, що дозволяє віддаленій точці доступу отримувати електричну енергію разом з даними через стандартну виту пару Ethernet-з'єднання. Ця технологія називається PoE (Power over Ethernet). Як уже згадувалося, такі пристрої доступу можуть бути налаштовані як з'єднання точка-точка (point-to-point) або як радіально-вузловий зв'язок - точка-мультиточка (point-to-multipoint). Завдяки особливостям реалізації вони дозволяють забезпечити зв'язок, що не вимагає ліцензування, в спектрі радіочастот Wi-Fi з дальністю близько 20 км. Однак таке використання неліцензійного спектра може спричинити і значні рівні перешкод. Проте подібні системи застосовуються постачальниками безпроводових інтернет-послуг в смугах 2,4 і 5 ГГц в міських і приміських районах.

Для приватних транзитних мереж таке рішення надає недорогий спосіб ретрансляції даних на великі відстані. Сполучення ретрансляційних станцій з локальною точкою доступу дає можливість швидкого і простого з'єднання з кластером пристроїв з підтримкою Wi-Fi у віддаленій області - наприклад, для рекреаційних або сільськогосподарських потреб. Хоча це має мінімальне відношення до потрібного для нас безпроводового Інтернету речей, подібне рішення може бути чудовим інструментом для побудови мереж з великим радіусом покриття від окремого пристрою. Але зі споживанням енергії вони, швидше за все, не будуть використовуватися як вузлові IoT-пристрої.

Найімовірніше, саме Wi-Fi залишиться однією з найпопулярніших технологій Інтернету речей в сегменті ринку обладнання для «розумного будинку», який стрімко розвивається. Він знаходить у цій галузі найширше застосування, оскільки має цілий ряд викладених вище переваг і в даному випадку практично не пов'язаний обмеженнями в частині енергоспоживання, які не характерні або не так критичні для інтелектуальних домашніх додатків з живленням від мережі напруги змінного струму. Що стосується Wi-Fi з малим енергоспоживанням, то загалом він буде використовуватися в тих додатках, яким достатньо періодичної передачі даних з низькою швидкістю. Це такі області застосування, як частина сенсорного обладнання та лічильники в «розумних будинках».

Однак потрібно пам'ятати, що у технології Wi-Fi є і недоліки. Крім високого енергоспоживання, існує ще цілий ряд проблем. Перша полягає в тому, що ця технологія, працюючи в спектрі частот, що не вимагає ліцензування, як наслідок, піддається підвищеному рівню перешкод через їх перевантаженість. Друга полягає в тому, що оскільки Wi-Fi може безпосередньо і без кабелю підключатися до Інтернету з усіма його погрозами, необхідно приділяти особливу увагу проблемам кібербезпеки. Пристрій Wi-Fi має бути спроектовано так, щоб забезпечити конфіденційність даних і правильну роботу кінцевого додатку. При масовій появі IoT-пристроїв через відсутність на багатьох з них браузерів і клавіатур їх підключення до Wi-Fi-мережі з точки зору налаштувань політики безпеки було спрощено. В результаті це призводить до атак DoT (DDoS of Things) на IoT-пристрої, і ця проблема все ще до кінця не вирішена.

З огляду на це питання, постачальникам Wi-Fi-обладнання необхідно приділяти більше уваги розробці програмних продуктів, які будуть гарантувати особливо це стосується Інтернету речей, що IoT-пристрої підключаються тільки по дозволеним портам і протоколам. При цьому ще додаються труднощі, пов'язані з хмарними технологіями, що широко впроваджуються. В Інтернеті речей доступ до хмарного сервера повинен бути безперебійним, і для цього Wi-Fi-мережі повинні стати ще більш безпечними - з можливістю цілодобового моніторингу, управління і самовідновлення.

Технологія Wi-Fi готова вже сьогодні підключити мільярди IoT-пристроїв один до одного, до Інтернету і до одиниць побутової електроніки, комп'ютерів і промислового устаткування. Висока стійкість Wi-Fi, його гнучкість і придатність для багатоцільового застосування, а також прихильність Wi-Fi до функціональної сумісності пристроїв, які використовують цю технологію, роблять Wi-Fi однією з ідеальних платформ для інновацій в безлічі технологій Інтернету речей.

### 2.2 Bluetooth, Bluetooth LE або Bluetooth Smart

Bluetooth як протокол зв'язку був розроблений ще в середині 1990-х років,

спеціально для організації персональних локальних мереж, що з'єднують різні пристрої, мобільні телефони, комп'ютерну периферію тощо. Bluetooth використовує діапазон 2,4 ГГц і спочатку був затверджений як стандарт IEEE 802.15.1. Зараз його просуванням займається спеціальна група Bluetooth Special Interest Group (Bluetooth SIG), яка є альянсом багатьох компаній, що створюють пристрої із застосуванням даної технології. Згодом стандарти Bluetooth диверсифікувались: за рахунок додавання в 2006 році Bluetooth Low Energy (BLE, Bluetooth LE, або Bluetooth Smart) і Bluetooth 5 в 2016 році.

Існує декілька типів поведінки цієї технології при радіозв'язку, тобто протоколів доступу до мультимедіа. Вони розроблені і легалізовані у вигляді стандарту Bluetooth SIG, і деякі з них несумісні з іншими протоколами Bluetooth MAC. MAC (Medium Access Control) - це підрівень управління доступом до середовища, який здійснює передачу фрагментів даних структури MAC за допомогою фізичного каналу. Технологія Bluetooth на фізичному рівні використовує GFSK-модуляцію (Gaussian Frequency-Shift Keying). Це вид частотної маніпуляції модуляцією, при якій застосовується фільтр Гаусса для згладжування позитивних і негативних частотних перебудов, що представляють собою бінарний інформаційний код - «1» або «0». Також Bluetooth може використовувати модуляцію з розширеним спектром FHSS (Frequency-Hopping Spread Spectrum), яка підвищує завадостійкість каналу зв'язку шляхом псевдовипадкової перебудови робочої частоти. В технології BLE застосовується метод прямої послідовності для розширення спектра DSSS (Direct Sequence Spread Spectrum). Ця технологія модуляції забезпечує високу продуктивність локальних безпроводових мереж шляхом розширення спектра випромінюваного сигналу. Вона полягає в підвищенні тактової частоти модуляції, при цьому кожному символу переданого повідомлення ставиться у відповідність досить довга псевдовипадкова послідовність. Останні протоколи Bluetooth мають функції запобігання впливу завад.

Технологія Bluetooth настільки популярна, що визначити область її типового використання досить важко. Вона досить поширена в безпроводових периферійних пристроях, призначених для ноутбуків і мобільних телефонів. Маються на увазі не

тільки безпроводові миші і гарнітури, але також фітнес-монітори і інші пристрої IoT. Крім того, останні версії протоколу здатні забезпечити більш широкий радіус зв'язку і знизити споживання енергії від батареї, а багато-які протоколи доступу до мультимедіа спрощують розробку інтелектуальної реклами, обміну ключами безпеки і дистанційного керування.

Профілі Bluetooth, протоколи, орієнтовані на додатки, мають безліч опцій меню: можна використовувати обмежений варіант - для додатків без встановлення з'єднання - або повний протокол, який дозволяє організувати безпечне з'єднання для надійної передачі даних, тобто з встановленням з'єднання. При останньому варіанті передача починається з даних виклику або з установки маршруту проходження пакетів від джерела до одержувача. Потім відбувається послідовна передача даних, і по її закінченні зв'язок розривається.

Деякі пристрої з Bluetooth, такі як принтери з живленням від мережі напруги змінного струму, використовують радіозв'язок ближнього радіусу дії для того, щоб виключити підключення кабелів, а не для обмеження споживання енергії. Однак для більшості пристроїв з живленням від батареї час їх автономної роботи є ключовим фактором, як правило, оптимальним є термін служби в десять років. Це не тільки дозволяє скоротити сервісні витрати на технічне обслуговування, пов'язане із заміною джерел живлення, але і робить використання таких пристроїв максимально комфортним.

Bluetooth Low Energy, званий також Bluetooth Smart для використання в IoT-пристроях, використовує переважно протокол BLE, який призначений спеціально для пристроїв з надмалим споживанням енергії. Якщо потрібна велика швидкість передачі в порівнянні з попередніми версіями Bluetooth, то можна застосувати Bluetooth 5, що пропонує більш швидку передачу і більш тривалі сеанси передачі на основі мережевого протоколу без встановлення з'єднання. В такому випадку дані, що надсилаються, містять повну адресну інформацію про відправника та одержувача в кожному пакеті. При передачі всі проміжні мережеві пристрої зчитують адресну інформацію і приймають рішення про маршрутизацію даних. Скорочення витрат енергії на радіозв'язок і оптимізація ПЗ націлені якраз на те, щоб

зробити десятирічний термін експлуатації без заміни елементу живлення, критичний для IoT, практично досяжним.

Завдяки широким можливостям по вибору доступних варіантів протоколів і економному використанню енергії акумулятора, технологію Bluetooth можна ефективно застосовувати і приймати як один з основних стандартів безпроводового зв'язку для IoT-пристроїв.

### 2.3 Технологія EnOcean

EnOcean - технологія безпроводового зв'язку Інтернету речей субгігагерцового діапазону, яка призначена для роботи без батареї. Живлення пристроїв Інтернету речей здійснюється за рахунок збору вільної енергії. Для цього використовується технологія "energy harvesting", яка використовує невеликі зміни в русі, тиску, світлі, температурі або вібрації для трансформації їх в придатну електричну енергію. Пристрої здійснюють передачу інформації зі швидкістю 120Кбіт / с на відстань до 100 метрів у вигляді пакетів даних з 14 біт.; аналогічно тому, як це працює в безпроводових брелоках, які відкривають замки дверей автомобіля, або в системах дистанційного керування гаражними воротами. Частота передачі для пристроїв становить 868МГц - неліцензуємий частотний діапазон.

Власником патентів і розробником технології є однойменна компанія EnOcean GmbH, дочірня компанія Siemens. Компанія Enocean GmbH виробляє передавачі, приймачі, трансивери і перетворювачі енергії для таких компаній як Thermokon, Wago, Omnio, Osram, Wieland Electric, Eltako, Distech Controls, Zumtobel, Peha, Herga, MK Electric та інших, які розробляють і виробляють кінцеві продукти.

EnOcean Alliance - це консорціум компаній Європи та Північної Америки, які розробляють і просувають безпроводові пристрої, які не потребують додаткового живлення. Консорціум був створений в 2008 році і спочатку включав компанії Enocean, Texas Instruments, Omnio, Sylvania, Masco і MK Electric. Вони заклали основу бездротових мереж автоматизації будівель.

Серед інших безпроводових технологій перевагою EnOcean є те, що вона не вимагає використання батарейок в своїх вимикачах і датчиках. Необслуговувані безпроводові вимикачі і безпроводові датчики істотно знижують вартість володіння системою і підвищують її надійність.

Міжнародна електротехнічна комісія (МЕК) ратифікувала безпроводовий стандарт Enocean - ISO / IEC 14543-3-10 - для безпроводових додатків з ультранизьким енергоспоживанням. Це перший і єдиний безпроводовий стандарт, який також оптимізований для рішень, які збирають енергію з навколишнього середовища. Разом з EnOcean Equipment Profiles (EEPs), розробленим альянсом EnOcean Alliance, цей міжнародний стандарт закладає основу для повністю сумісних, відкритих безпроводових технологій, таких як Bluetooth і WiFi.

Стандарт Enocean орієнтований на безпроводові сенсори, датчики і безпроводові сенсорні мережі з ультранизьким енергоспоживанням. Він також включає в себе і сенсорні мережі, які використовують технології добування енергії з навколишнього середовища, наприклад, від руху, світла або різниці температур. Цей принцип дозволяє сенсорам і їх електронним системам управління працювати незалежно від зовнішніх джерел живлення.

Міжнародна стандартизація дозволить прискорити розробку та впровадження енергетично оптимізованих безпроводових сенсорів і безпроводових сенсорних мереж. Міжнародне визнання технологій відкриває нові ринки і сфери застосування для рішень, які отримають енергію з навколишнього простору. Технологія EnOcean доповнює вже усталені системи автоматики для дому та промисловості. Вона призведе до розвитку в майбутньому таких застосувань, як Розумний Дім і Інтелектуальна Будівля, до рішень для промисловості, логістики і транспорту.

Членами альянсу EnOcean Alliance вже розроблено понад 850 сумісних продуктів, що відповідають стандарту Enocean. Розробники і виробники можуть отримати вигоду з обширного практичного досвіду альянсу, величезного асортименту, досвіду інсталяцій і багатьох років навчання користувачів. Альянс EnOcean Alliance розробляє профілі для додатків (EPPs), які забезпечують сумісність продуктів різних виробників. Вони оптимізовані для ультранизького

споживання енергії і є ідеальним, випробуваним доповненням до нових стандартів безпроводового зв'язку. Це означає, що розумні, енергетично ефективні рішення в області автоматизації можуть бути реалізовані незалежно від виробника в будь-якій галузі промисловості. Безпроводові технології EnOcean вже міцно утвердилися, як технології для екологічних, інтелектуальних будівель і додатків. Альянс EnOcean Alliance бачить ратифікацію міжнародного стандарту ISO / IEC 14543-3-10 як одну з ключових передумов для розширення вже досить успішних, швидко зростаючих EnOcean-екосистем.

### 2.4 Технологія LoRaWAN

LoRa (Long Range) - це досить новий метод модуляції і однойменна мережева технологія, що просувається відкритою некомерційною організацією LoRa Alliance. У альянс входять багато провідних гравців ринку Інтернету речей: IBM, Semtech, Cisco, Inmarsat, Swisscom та інші. Технологія LoRa має дещо інший характер, ніж всі описані раніше протоколи безпроводового зв'язку малого радіусу дії.

Як правило, під LoRa зазвичай мається на увазі тип модуляції, а під LoRaWAN - відкритий мережевий протокол LoRa, який не треба безпосередньо асоціювати з LPWAN. LoRaWAN використовується для передачі невеликих за обсягом пакетів даних на дальні відстані. Така мережа була розроблена спеціально для розподілених мереж телеметрії, міжмашинної взаємодії і Інтернету речей. Мережа LoRa є однією з перспективних безпроводових технологій, що забезпечують середовище збору даних з різного устаткування: датчиків, лічильників та сенсорів.

Залежно від регіональних розподілів, в такій мережі використовуються радіочастоти субгігагерцового діапазону в які не потребують ліцензування в спектрах частот в діапазонах VHF (30-300 МГц), UHF (300 МГц - 3 ГГц) або 800-930 МГц. Оскільки технологія LoRa застосовує більш низькі радіочастоти, ніж стандарти, що використовують частоти 2,4 або 5 ГГц, вона відрізняється від них і по радіочастотним характеристикам, при цьому сигнали LoRa можуть проникати глибоко в будівлі і в місця, недоступні більш високочастотним сигналам.

Модуляція LoRa сильно виділяється на фоні інших типів модуляції, і є справжнім досягненням в області радіочастотних технологій. Більшість стандартів ближнього радіусу дії, як було сказано раніше, використовує той чи інший різновид модуляцій FSK, OFDM, FHSS або DSSS з розширенням спектру. LoRa - це набір методів модуляції, запатентованих компанією Semtech, з розширенням спектра за допомогою лінійної частотної модуляції - Chirp Spread Spectrum (CSS). В цілому суть цього підходу полягає в перебудові несучої частоти за лінійним законом.

Завдяки такій перебудові сигнал отримує високий рівень завадостійкості. Крім того, при такому методі розширення спектра низькі бітові швидкості (до 300 біт/с) можуть уникнути впливу джерел вузькосмугових перешкод, таких як FSK-сигнали, і успішно відновитися на приймальному кінці. Це може дати лінії зв'язку LoRa перевагу в 15 дБ у порівнянні з вузькосмуговим FSK-сигналом при використанні радіочастотних сигналів однакової потужності. Що стосується шумів, то LoRa може прекрасно і без проблем працювати нижче рівня навколишнього радіочастотного шуму і на 20 дБ або навіть ще нижче по відношенню до вузькосмугових джерел завад – через посилення, властивого цьому виду модуляції з розширеним спектром.

Також технологія LoRa дозволяє використовувати різні комбінації швидкості передачі даних і модуляції. Вони можуть бути обрані виходячи з різних міркувань: наприклад, для збільшення швидкості передачі даних (до 40 Кбіт/с) з меншим діапазоном покриття, коли саме швидкість передачі є критичним фактором, або для досягнення більшої дальності зв'язку з низькою радіочастотною потужністю в зашумлених середовищах. Справа в тому, що при зниженні швидкості передачі даних на один біт доводиться більше енергії і його легше розпізнати на приймальному кінці - отже, при одній і тій же споживаній потужності і чутливості приймача дальність зв'язку збільшується. Цікаво, що коефіцієнти розширення спектра LoRa, звані SF (Spreading Factor), при передачі даних можуть бути активні в одному каналі, не заважаючи при цьому один одному. Оскільки сигнал CSS простіше декодувати, ніж сигнали з іншими технологіями розширення спектра, то це можна зробити і з меншою обчислювальною потужністю. Що, в свою чергу,

призводить до збільшення часу автономної роботи пристроїв Інтернету речей, незважаючи на більш складне рішення в частині модуляції.

Мережа LoRa може бути розгорнута або як окрема мережева архітектура, або як зв'язана мережа в тих районах земної кулі, де є оператори мережі загального користування, які за плату забезпечують можливість пристроїв LoRa підключатися через шлюзи для передачі даних в хмару. Мережа на основі технології LoRa вперше була розгорнута в Європі, але вона успішно поширюється і на інші регіони. Крім компанії Semtech, мікросхеми LoRa у вигляді систем на кристалі виробляють ST Micro і Microchip, що дає розробникам певну гнучкість в реалізації проектів на базі технології LoRa.

Проте не можна забувати, що при застосуванні даної технології, навіть якщо використовується спектр частот, який не вимагає ліцензування, необхідні сертифікація пристроїв і підтвердження того, що конкретний пристрій дійсно відповідає специфікації LoRa. Для сертифікації зазвичай потрібні випробування на потужність передавача, девіацію частоти, займану смугу пропускання, гармоніки і спектральну щільність потужності. Сертифікацію LoRa і попереднє тестування вже забезпечує цілий ряд авторизованих випробувальних лабораторій.

Незважаючи на те, що LoRa - це досить новий стандарт для розробників, їм доступні і мікросхеми, і готові модулі, і різні тестові інструменти[6].

### 2.5 Технологія ZigBee

Ця технологія є ще одним вдалим рішенням, яке орієнтоване на додатки, що вимагають гарантованої безпечної передачі даних при відносно невеликих швидкостях. Вона забезпечує можливість тривалої роботи мережевих пристроїв від автономних джерел живлення (батарей). Мережі, утворені за протоколом ZigBee, почали привертати увагу ще з 1998 року, коли багато розробників усвідомили, що протоколи Wi-Fi і Bluetooth стали недостатньо ефективними для цілого ряду додатків. Зокрема, багато інженерів побачили необхідність в самоорганізованих мережах. У такій тимчасовій мережі вузли можуть зв'язуватися безпосередньо,

точка-до-точки, без потреби в спільній точці доступу. Технологія ZigBee використовує радіочастоти, які не потребують ліцензування ISM-діапазону, включаючи смугу в районі 2,4 ГГц. Однак в різних регіонах і країнах для цього стандарту зв'язку застосовуються різні смуги робочих частот: так, в США для ZigBee виділена смуга в субгігагерцовому діапазоні, що включає 915 МГц, в Китаї це 784 МГц, а в Європі - 868 МГц. Протокол ZigBee спочатку підтримує мережеві з'єднання типу «дерево», «зірка» і мережі, що самоорганізовується з комірчастою топологією, які призначені для вирішення широкого кола завдань. Підключені таким чином пристрої для керування вузлами можуть передавати дані через канали зв'язку в мережу, що робить технологію ZigBee більш привабливою (в порівнянні з мережею «точка-точка» в аналогічних умовах) для організації мереж з низькою швидкістю передачі даних, розподілених по великій площі.

Плата за всі переваги ZigBee - це скорочення часу автономної роботи пристроїв, які служать репітерами кластерів такої мережі, які використовуються в процесі обміну даними з більш віддаленими IoT-пристроями. Прискорене виснаження енергії батарей пов'язано з тим, що пристроям доводиться передавати не тільки свої власні дані і підтвердження між вузлами мережі, але також дані і підтвердження з інших пристроїв. Що ж стосується завадостійкості, то хоча розширена специфікація від 2007 року, яка отримала назву ZigBee Pro, надає можливість використання технології з перескоком частоти, проте в цьому випадку при наявності завад переходити на інший канал має відразу вся мережа. Якщо говорити про швидкість передачі, то в залежності від області застосування пристрою вона може перебувати в діапазоні від 10 до 250 Кбіт/с.

Хоча невисокі швидкості можуть бути цілком достатніми для багатьох IoT-пристроїв, необхідно брати до уваги, що при використанні технології ZigBee ви маєте меншу пропускну здатність каналу, ніж при протоколах Wi-Fi. Нижчі швидкості зазвичай означають і більш економне використання енергії батареї, яка витрачається на процесори, логічні мікросхеми і, звичайно, передачу. Характерна для даної сфери застосування та діапазону частот низька швидкість передачі даних при нечастих оновленнях даних може забезпечити пристрою більш тривалий

термін служби батареї. А це зараз є досить привабливою і конкурентною властивістю на ринку технологій «Інтернету речей».

В даний час технологія Zigbee використовується в багатьох додатках самого різного призначення, які вимагають підключення з малою витратою споживаної потужності, включаючи домашню автоматизацію і промислові мережі. Наприклад, замок «без ключа» на вхідних дверях і регулятор температурного режиму цілком можуть бути пристроями ZigBee.

Профілі додатків, що представляють собою протоколи більш високого рівня і бібліотеки для різних цілей і областей застосування, які полегшують організацію взаємодії між пристроями ZigBee від декількох постачальників, визначає альянс ZigBee Alliance.

Зв'язок в мережі ZigBee здійснюється за допомогою передачі пакетів даних між підключеними до мережі пристроями, які бувають трьох видів:

- координатор (ZC);
- маршрутизатор (ZR);
- кінцевий пристрій (ZED).

Координатор ініціалізує мережу і керує її процесами: задає і зберігає ключі безпеки пристроїв, встановлює політику безпеки своєї мережі і з'єднується з іншими мережами. Координатор в кожній мережі ZigBee може бути тільки один.

Порівняємо між собою технології Wi-Fi, Bluetooth та ZigBee(таблиця 2.1):

Таблиця 2.1 – Порівняння технологій

| Технологія | Wi-Fi | Bluetooth | ZigBee |
|---|---|---|---|
| Стандарт зв'язку | IEEE 802.11 | IEEE 802.15.4 | IEEE 802.15.4 |
| Швидкість передачі даних | 300+ Мбіт/с | до 3 Мбіт/с | до 250 Кбіт/с |
| Енергоспоживання | високе | низьке | низьке |
| Підтримка IP | так | ні | ні |
| Топологія | «зірка» | «зірка» | «mesh» |

З мінусів можна відзначити низьку швидкість передачі даних - до 250 кбіт/с.

Заради низького енергоспоживання, доводиться чимось жертвувати, але це не критично для задач домашньої автоматизації.

### 2.6 Технологія Z-Wave

Z-Wave є безпроводовим протоколом зв'язку, розробленим для домашньої автоматизації, зокрема для контролю середовища та управління житловими будинками, а також комерційними об'єктами. Ця технологія дає можливість безпечно обмінюватися короткими фрагментами даних на радіочастотах діапазону ISM до 1 ГГц і дозволяє розширювати діапазон передач при низькій споживаній потужності. У Z-Wave використовується FSK- або GFSK-модуляція, і хоча ця технологія спочатку була запатентована, в даний час вона є загальнодоступною відкритою специфікацією ITU G.9959.

Технологія Z-Wave розвивається і підтримується компанією Sigma Design, відомим виробником напівпровідникових пристроїв і мікросхем. Z-Wave - це набір пропрієтарних протоколів фізичного, що визначають на якій частоті працює мережа, рівень сигналу, що передається, його модуляцію тощо, і логічного, такі протоколи задають адресацію пристроїв, набір команд, послідовність обміну інформацією тощо, рівня, реалізованих в декількох наборах мікросхем Sigma Design.

«Пропрієтарна» - в даному випадку означає, що вся документація, яка детально описує протоколи - закрита, а кожен виробник, який хоче розробляти пристрої, керовані за технологією Z-Wave повинен підписати сувору угоду про нерозголошення деталей протоколу. Безумовно, такий підхід накладає певні обмеження, але в той же час є і важлива перевага - абсолютно всі пристрої, з підтримкою Z-Wave гарантовано сумісні між собою. Тобто, яким би не був випущений датчик або центральний контролер, він майже напевно буде працювати з будь-яким іншим пристроєм, яке орієнтоване на роботу в мережі Z-Wave. Майже – тому що в декількох випадках, виробники можуть програмно обмежити підтримку до продуктів тільки одного бренду. Але в цілому, такий підхід в «команді

Z-Wave» не популярний.

Мережа Z-Wave на фізичному рівні організована за принципом mesh-мережі. Mesh, в перекладі з англійської означає «сітка, стільники». У звичних нам мережах, наприклад, мережах Wi-Fi, кожен пристрій, що працює в мережі має бути безпосередньо пов'язаний з центральним контролером, в разі Wi-Fi - з Wi-Fi-роутером – такий спосіб організації мережі зазвичай називають «зіркою». Якщо рівень сигналу контролера або кінцевого пристрою занадто малий, щоб забезпечити такий прямий зв'язок, значить такий пристрій підключити буде неможливо.

У мережах Mesh - кожен компонент мережі завжди виступає в якості своєрідного ретранслятора сигналу – це означає, що навіть якщо якийсь датчик або актуатор не може безпосередньо підключитися до хабу «розумного будинку» через слабкий сигнал, а саме такий рівень сигналу передбачається до використання в безпроводовій мережі «розумного будинку», але «бачить» якийсь інший датчик або компонент мережі Z-Wave - він може бути підключений до мережі і центральний контролер зможе ним керувати. Таким чином, незважаючи на невеликі значення потужності радіосигналу в мережі Z-Wave - вона може покривати значні відстані і масштабні об'єкти наприклад, багатоповерхові будівлі.

Серед інших важливих переваг технології Z-Wave можна відзначити такі:

- легке підключення в мережу: для того, щоб підключити датчик або актуатор до мережі Z-Wave досить на пару секунд натиснути одночасно на контролері і на самому пристрої невелику кнопку - це все, що необхідно;
- високий рівень безпеки: всі повідомлення в мережі Z-Wave шифруються за допомогою криптостійкого 128-бітного ключа. З огляду на те, що сигнал мережі Z-Wave практично неможливо зловити поза приміщенням, де розгорнута безпроводова мережа - зламати Z-Wave «зовні» практично неможливо. Це підтверджують практики кіберзлочинності – незважаючи на багаторічні спроби, отримати несанкціонований доступ до мережі «розумного будинку», побудованого на базі Z-Wave, так і не вдалося;
- офіційно дозволений діапазон: Протокол Z-Wave працює в частотному діапазоні (869 МГц), який офіційно дозволений для використання

пристроями з малою величиною радіосигналу. У різних країнах, діапазон частот, виділених під малопотужні мережі датчиків і актуаторов відрізняється.

При створенні розумного будинку в рамках окремої квартири використання «чужих» частот приховує в собі лише одну істотну неприємність: в майбутньому, якщо користувач вирішить додати в мережу додаткові датчики або актуатори, він може зіткнутися з тим, що компонентів з потрібною йому частотою не буде в продажу, наприклад, будуть зроблені загороджувальні заходи щодо імпорту та продажу пристроїв з невирішеними до побутового використання частотами. Але отримати штраф йому навряд чи загрожує, як ми вже говорили, рівень сигналу в мережі Z-Wave занадто малий і практично не виявляється поза межами приміщення.

Проте, при проектуванні більших об'єктів, комерційних інсталяцій, готелів, багатоквартирних будинків ми рекомендуємо звертати пильну увагу на робочу частоту встановлюваних пристроїв і вибирати компоненти Z-Wave, які орієнтовані на ринок – щоб в подальшому не виникало проблем з сумісністю і органами державного нагляду за використанням радіо частотного ресурсу.

### 2.7 Технологія Jeweller

Jeweller – це безпроводова технологія радіозв'язку.

Надійна охоронна система потребує стабільного і постійного зв'язку. Але швидкісний і якісний інтернет є далеко не скрізь. Тому сигналізація компанії AJAX спроектована таким чином, щоб гарантувати безпеку об'єкту, що охороняється, а також можливість віддаленого контролю і управління всією системою навіть при невисокій якості зв'язку. Дуже компактний IoT-протокол AJAX дозволяє охоронній системі нормально функціонувати навіть при швидкості Інтернет-з'єднання GPRS 0,5 Кбіт/сек.

Завдяки двом антенам AJAX Hub аналізує рівень сигналів в режимі реального часу і вибирає найкращий. У разі саботажу всієї смуги або злому датчика Hub

негайно підніме тривогу.

Опитування і перевірка зв'язку з датчиками виконується кожні 12 секунд. Навіть якщо зв'язок зник, система повідомить про тривогу за допомогою алгоритму DeliverAnyway. Всі дані, які передаються всередині охоронної системи або в хмару, надійно шифруються з використанням алгоритму на основі AES. На злом піде дуже велика кількість часу. Також до централі (Hub) можна підключити до 100 пристроїв, тобто датчики можна встановити в кожну кімнату величезного будинку, а також на кожні двері і вікно.

Датчики Ajax працюють на відстані до 2 000 метрів відкритого простору від хаба. У приміщеннях ця дальність гарантує, що зміна планування або перестановка меблів не зможуть порушити зв'язок. Сигнал все одно буде доставлений до хабу.

Створити потужну систему нескладно – важче забезпечити її безперебійну роботу. Технологія Jeweller підтримує мінімально необхідний рівень вихідної потужності і економить заряд батареї. Завдяки цьому датчики Ajax стабільно працюють до 7 років.

Ajax Hub завжди знає, на зв'язку датчик чи ні. Двосторонній зв'язок, адресність і перевірка пристроїв з інтервалами від 12 секунд гарантують цілісність системи. Якщо один з датчиків вийде з ладу або буде зламаний, Ajax миттєво повідомить про неполадку і її причини.

Щоб уникнути глушіння датчиків від накладення радіохвиль, в корпус централі вбудовані дві антени. Ajax Hub в реальному часі аналізує рівень сигналів і приймає кращий. Так зв'язок з датчиками підтримується навіть в екстремальних радіо умовах.

Використання однієї частоти в роботі безпроводової системи безпеки недостатньо надійно, тому Ajax працює на кількох. У разі глушіння алгоритм перемикає систему на чисту частоту. Якщо заглушена вся смуга, Hub підніме тривогу.

Нижче вказані основні технічні характеристики:

- потужність радіосигналу: до 25 мВт;
- тип зв'язку: двосторонній;

- робочі частоти: 868.0-868.6 МГц;
- тип шифрування: блочне, на основі алгоритму AES;
- дальність зв'язку з датчиками: до 2000 метрів на відкритій місцевості;
- період опитування датчиків: від 12 секунд;
- максимальна кількість підключених пристроїв: до 100;
- термін роботи датчиків при щохвилинних пінгах: до 7 років;
- час доставки сигналу тривоги: миттєво;
- додатково: TDMA, захист від глушіння, захист від підробки, захист від збоїв, віддалене налаштування.

Система безпеки Ajax самодостатня. Hub відстежує появу нової версії програмного забезпечення, автоматично завантажує і встановлює оновлення. Інсталятору не потрібно виїжджати на об'єкт, налаштування можливе з будь-якої точки на Землі[11].

**Висновки до розділу**

1. В даному розділі проаналізовано основні безпроводові технології, які вирішують питання організації мереж IoT як на низькому рівні з малою зоною власного покриття, так і для передачі інформації на великі відстані.

2. Характерною особливістю мультисервісних мереж є наявність електроживлення на кожному об'єкті, що підключається. І проблема забезпечення електроживлення датчиків стоїть дуже гостро, ускладнюючи застосування радіотехнологій. Для вирішення цієї проблеми застосовуються стандарти підключення розумних пристроїв, що мають підвищену живучість і розроблені для мінімізації енергоспоживання, – 6LoWPAN, Bluetooth Low Energy (BLE), ZigBee, Z-Wave, EnOcean, Jeweller тощо.

# 3 СТРУКТУРА ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ ОХОРОННИХ СИСТЕМ ТА СИСТЕМ ОБМЕЖЕННЯ ДОСТУПУ

## 3.1 Системи обмеження доступу для офісних приміщень

Система контролю і управління доступом - це повнофункціональний електронний вузол, який виступає в якості буфера між зчитуючими пристроями і функціональними механізмами. Якщо вказати простіше СКУД це універсальний засіб, який збирає, аналізує і обробляє величезну кількість інформації в приміщенні і приймає рішення на предмет надання доступу в тих, чи інших ситуаціях.

Системи контролю доступу (СКУД) - важливий елемент системи безпеки, як на великих підприємствах, так і в маленьких офісах. Це ефективне рішення для захисту будівлі або приміщення від несанкціонованого проникнення. Також системи контролю доступу дозволяють вести облік робочого часу персоналу, розмежовувати доступ в приміщення, складати звіти про переміщення співробітників. При цьому участь людини мінімізовано.

Система контролю і управління доступом, або СКУД - це сукупність різних елементів (устаткування та комплектуючі, ПЗ), які забезпечують контроль і управління доступом до певного об'єкту. Основна функція такого рішення - управляти доступом на певну територію, тобто обмежувати його для сторонніх і/або небажаних осіб, а також ідентифікувати осіб, які мають доступ до підприємства.

Сучасний контролер СКУД має величезний функціонал. Він може як просто зчитувати біометричні дані з сенсора двері і дати доступ конкретній особі, так і працювати складному режимі:

- не допускати в приміщення кількість людей більше встановленого;
- давати вибірковий доступ певним людям в різний час доби, чи пори року;
- зчитувати інформацію з приміщення і при потребі включати режим "тривоги", якщо протягом певного часу не буде зареєстровано ознаки руху;
- ведення бази співробітників компанії і відвідувачів;

- облік робочого часу;
- об'єднання з системою безпеки (з відеокамерою, сигналізацією).

Іншими словами: системи контролю вкрай адаптивні, різнобічні і можуть бути налаштовані виключно на ваш розсуд. Вищевикладений список це далеко не повний перелік всіх можливостей сучасних систем контролю доступу. Це проста демонстрація найбільш простих функцій, які ви отримаєте при використанні СКУД.

При використанні даних систем в "офісному режимі" вам стають доступні опції з контролю обліку робочої діяльності всіх авторизованих співробітників, що значним чином підвищує рівень дисциплінованості і веде повний облік пересування всіх людей всередині вашої організації. До всього іншого з'являється можливість автоматизації обліку робочого дня, що дозволить вам заощадити на витратах знявши цю функцію з відповідного відділу.

Найбільш примітним є той факт, що дане рішення в останні роки користується все більшою популяризацією в приватному секторі. Пояснюється це простим зменшенням вартості технології на ринку. Те, що раніше могли собі дозволити лише великі корпорації, сьогодні є доступними звичайній людині. Якщо раніше СКУД стояв лише на сторожі промислових секретів великих конгломератів, то сьогодні ця ж система може повністю забезпечити ваш будинок від неприємних проникнень на приватну територію. Особливо ефективно дане рішення працює в парі з охоронними системами.

Чи варто вам купити сучасну систему контролю управління доступом, або покластися на більш консервативні методи охорони власного майна - виключно ваш вибір. Але в 98,2% випадків використання систем контролю доступу злочинні дії спрямовані на проникнення всередину контрольованої СКУД території були припинені різними методами, в тому числі і за допомогою своєчасної передачі обробленої інформації відповідним органам.

Переваги СКУД очевидні - їх використання мінімізує участь людини в контролі доступу, вони працюють цілодобово, дозволяють вести облік робочого часу для підтримання дисципліни в компанії.

### 3.1.1 Елементи СКУД

Системи контролю доступу в приміщення або іншу задану територію можуть включати такі елементи:

- перегороджуючі пристрої (до них відносяться електромагнітні та електромеханічні замки, шлагбауми, ворота, турнікети);
- ідентифікатори: картки або брелоки, які використовуються для отримання доступу в приміщення. Ідентифікатором також може бути код, який відвідувач вводить на клавіатурі, або біометричні дані (наприклад, відбиток пальця)();
- контролери(Рисунок 3.1): контролер являє собою серце СКУД, адже саме цей пристрій визначає, чи надати доступ власнику ідентифікатора (карти, відбитка пальця тощо);
- зчитувачі(Рисунок 3.4): «зчитують» дані з ідентифікатора і передають їх контролеру;
- термінали(Рисунок 3.2, Рисунок 3.3): багатофункціональні пристрої, що поєднують в одному корпусі зчитувач і контролер;
- ПЗ: спеціальний софт необхідний, якщо потрібна обробка отриманих зчитувачем даних для формування звітів або для початкового програмування і управління системою.


Рисунок 3.1 - Мережевий контролер доступу на 2 двері


Рисунок 3.2 – Приклад біометричного терміналу MultiBio 700


Рисунок 3.3 - Біометричний Wi-Fi термінал

Рисунок 3.4 - Зчитувач безконтактний

### 3.1.2 Класифікація СКУД

Існує два основних типи систем біометричного контролю доступу:

- автономні (їх також називають локальними);
- мережеві.

Перші кращі для маленьких офісів, другі підійдуть для великих компаній з великою кількістю приміщень. Автономна СКУД передбачає управління однією/декількома точками доступу, немає передачі на центральний пульт, немає контролю оператора і не використовується керуючий комп'ютер. У свою чергу, мережева система передбачає управління великою кількістю точок доступу і з'єднання всіх контролерів з керуючим комп'ютером.

Також СКУД класифікують за кількістю контрольованих точок:

- СКУД малої місткості (до 16 точок доступу);
- СКУД середньої місткості (від 16 до 64 точок доступу);
- СКУД великої місткості (понад 64 точок доступу).

## 3.2 Охоронні системи для житлових приміщень

Перші системи охоронної сигналізації з'явилися більше ста років тому. Це абсолютно не дивно, адже протягом всієї історії свого існування людина постійно прагнула вберегти своє майно від зазіхань зловмисників. Особливої актуальності охоронні системи набули в наш час. Промислове шпигунство, загроза викрадення конфіденційної інформації або обладнання, квартирні крадіжки, ось далеко не повний перелік проблем, з якими стикається сучасне суспільство.

Спочатку сигналізація представляла собою простий пристрій, принцип якого полягав в розмиканні або замиканні контактів при спробі проникнення в приміщення, з подальшим спрацьовуванням звукового оповіщення. Сучасні системи сигналізації є високотехнологічним комплектом обладнання, що має велику кількість різноманітних функцій і можливостей.

Як правило, система сигналізації складається з таких компонентів:

- Керуючий блок;
- Датчики руху;
- Датчики розбиття скла;
- Датчики відкриття дверей;
- Сирена;
- Датчики контролю периметра.

### 3.2.1 Безпроводовий датчик розбиття скла

Безпроводовий датчик розбиття скла призначений для виявлення розбиття скла в приміщенні, що охороняється. Завдяки спеціальному мікрофону датчик виявляє і реєструє специфічні низькочастотні і високочастотні звуки, що виникають при розбитті скла. У разі, якщо в приміщенні, що охороняється розбивають скло, датчик виявляє ці звуки і надсилає по радіоканалу сигнал тривоги на центральний блок сигналізації. Використовуючи унікальний багатоступінчастий аналіз, датчик реагує виключно на звук розбитого скла, ігноруючи інші гучні звуки.

Датчик може використовуватися для виявлення розбиття скла в квартирах, будинках, магазинах, офісних будівлях, готелях, ресторанах, банках, школах, студіях, на складах, тощо. Перевагою датчика є і його зручне і надзвичайно легке самостійне встановлення за допомогою смарт-кріплення, для монтажу користувачеві не потрібно розбирати сам датчик.

Датчик оснащений ефективною безпроводовою системою радіозв'язку, яка використовує шифрування повідомлень і захист від підробки. Це забезпечує чудову захищеність сигналізації від спроб злому. Крім того, датчик має ультрасучасну високонадійну систему зв'язку, що дозволяє йому успішно працювати в межах декількох поверхів бізнес-центру або на відстані до 2000 м на відкритій місцевості від центрального блоку сигналізації.

Рисунок 3.5 – Безпроводовий датчик розбиття скла

### 3.2.2 Безпроводовий датчик відкриття дверей/вікна

Безпроводовий датчик відкриття дверей/вікна призначений для детектування відкриття дверей, вікон тощо. Датчик обладнаний клемною колодкою для підключення додаткових проводових датчиків, в тому числі проводових датчиків відкриття призначених для встановлення на металеві ворота і люки.

Конструкція датчика складається з двох частин - магніту і блоку з герконом. Передбачено два варіанти магніту - для паралельного (великий магніт) і перпендикулярного (малий магніт) встановлення.

Принцип роботи датчика відкриття заснований на властивостях геркона, здатного ставати провідником під впливом магнітного поля. У нормальному стані магніт і блок з герконом зімкнуті. Як тільки двері, на яких встановлено датчик, відкриваються - магніт віддаляється від геркона, контакти розмикаються і геркон перестає проводити струм. При закритті дверей відбуваються зворотні процеси: магніт наближається до геркона, контакти замикаються і геркон починає проводити струм. В обох випадках датчик спрацьовує і миттєво відсилає повідомлення про тривогу на центральний блок.

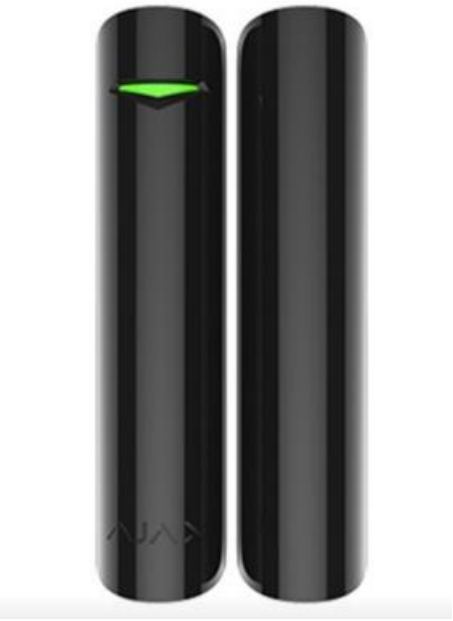


Рисунок 3.6 - Безпроводовий датчик відкриття дверей/вікна

### 3.2.3 Безпроводовий датчик руху

Датчик має регульовану чутливість і здатний ігнорувати домашніх тварин вагою до 20 кг і зростом до 50 см. Принцип дії датчика заснований на визначенні інфрачервоного (ІЧ) випромінювання від живої істоти. Кожна жива істота, в тому числі осіб - джерело ІЧ випромінювання. Як тільки датчик зауважує таке випромінювання, він аналізує масу живого об'єкта, і в разі, якщо вона перевищує 20 кг, відсилає сигнал тривоги на центральний блок охоронної сигналізації по радіоканалу. Спеціальний алгоритм обробки сигналу забезпечує додаткову перевірку об'єкта з приводу маси і наявності руху, мінімізує помилкові спрацьовування від переміщення домашніх тварин. Таким чином датчик спрацьовує тільки при виявленні руху людини. Також датчик не реагує на переміщення неживих предметів. Якщо в приміщенні, наприклад, впаде з вішалки куртка, або протяг відкриє міжкімнатні двері, датчик не спрацює.

Рисунок 3.7 – Безпроводовий датчик руху

### 3.2.4 Безпроводова вулична сирена

Безпроводова вулична сирена призначена для візуального та звукового оповіщення про тривогу. При тривозі, розумна централь сигналізації(Hub) передає радіо-сигнал на сирену. Після отримання сигналу тривоги від централі сирена спрацьовує і лунає сигнал тривоги.

Рисунок 3.8 – Безпроводова вулична сирена

### 3.2.5 Безпроводовий датчик виявлення диму та чадного газу

Безпроводовий датчик виявлення диму та чадного газу призначений для виявлення пожежі в приміщенні, що охороняється. Датчик виявляє дим, чадний газ

за допомогою інфрачервоного випромінювача і фотоприймача. Елементи змонтовані в спеціальній димовій камері. При потраплянні частинок диму в камеру, фотоприймач виявляє спотворення інфрачервоного променя. Якщо диму стає багато, спотворення променя стає сильним, датчик відправляє радіо-сигнали про пожежну тривогу на розумну централь (Hub) і включається сирена. Також датчик реагує на різке підвищення рівня температури, навіть в незадимлену приміщенні, і аналогічним чином відправляє тривожний сигнал.


Рисунок. 3.9 - Безпроводовий датчик виявлення диму та чадного газу

### 3.2.6 Брелок для керування охоронною системою

Брелок призначений для дистанційного встановлення на охорону сигналізації і зняття з охорони. При натисканні певної кнопки брелок по радіоканалу відправляє сигнал на центральний блок сигналізації. Централь обробляє сигнал і включає або відключає режим охорони. Брелок оснащений спеціальною кнопкою тривоги, при її натисканні центральний блок негайно перейде в режим «тривога». Також кнопки брелока можна запрограмувати для управління пристроями розумного будинку. Працює на відстані до 800 м.

Рисунок 3.10 – Брелок для керування охоронною системою

### 3.2.7 Розумна централь (Hub)

Інтелектуальний центр мережі примножує можливості кожного пристрою. Контролює їх роботу і збирає дані за допомогою технології безпроводового зв'язку Jeweller. Аналізує загрози, відкидує помилкові спрацьовування і повідомляє вам про випадки реальної небезпеки.

Захищеність від збоїв та зручна експлуатація:

- Система працює навіть при дуже поганій якості зв'язку: достатньо швидкості GPRS 0,5 кбіт / сек;
- Двосторонній зв'язок з пристроями дає можливість постійного тестування і простого налаштування;
- Прошивка і софт оновлюються автоматично;
- Можливе керування брелоком або за допомогою додатків для смартфона (iOS/Android) або через браузер;
- Підтримувані платформи для мобільних додатків: iOS 7.1 і вище, Android 4.1

і вище;

- Hub зберігає історію всіх зазначених системою подій;
- Перегляд в реальному часі відео потоку з відеокамер, які підтримують протокол RTSP.
- Всі роз'єми і кнопки заховані в корпус;
- При відключенні зовнішнього електроживлення включається тривога;
- Час роботи на резервному живленні досягає 15 годин;
- Відгук датчиків перевіряється пінгуванням частотою від 12 секунд;
- Працюють системи виявлення та запобігання глушіння, шифрування каналів, аутентифікації для захисту від підробки пристроїв;
- Для зв'язку з кожним пристроєм мережі хаб використовує вільну частоту і перебудовується в разі збігу;
- Модуль GSM дає резервний канал зв'язку на випадок відключення інтернету.


Рисунок 3.11 – Розумна централь(Hub)


Рисунок 3.12 – Комплект сигналізації

Залежно від потреб підприємства чи приватної особи система сигналізації може бути побудована з компонентів різних виробників, або встановлений готовий розширюваний комплект сигналізації. Велику популярність серед представників малого бізнесу, а також приватних клієнтів набувають бездротові комплекти сигналізації, які мають можливість подальшого розширення.

Головними перевагами системи сигналізації для будинку є простота установки, налаштування, а також широкий функціонал пристроїв даного типу. Комплект бездротової сигналізації може бути встановлений і налаштований покупцем самостійно, для цього не потрібно якихось специфічних знань і умінь. Весь процес монтажу і налаштування описаний в інструкції.

Сучасні бездротові системи охорони та сигналізації мають велику кількість корисних функцій і особливостей. Найбільш популярними з них є:

- Можливість управління сигналізацією через смартфон;
- Автоматичне оновлення прошивки і програмного забезпечення;
- Передача даних по засобам мереж GSM і Ethernet;

- Низькі вимоги до каналу зв'язку;
- Тривалий час роботи бездротових датчиків від живлячої елемента;
- Підключення до моніторингу великої кількості користувачів;
- Можливість підключення нового пристрою за допомогою QR-коду.

При необхідності купити систему охоронної сигналізації необхідно дотримуватися кількох простих рекомендацій. В першу чергу потрібно вирішити, який об'єкт буде ставиться на охорону. Виходячи з цього можна визначити необхідну кількість датчиків, а також їх тип. Охоронна сигналізація може бути, як провідний, так і бездротової. Кращим рішенням для будинку і квартири є бездротова система сигналізації. Її датчики і пристрої мають стильний зовнішній вигляд, а відсутність проводів позбавить від необхідності прокладки зайвих комунікацій[12].

### 3.3 IP відеоспостереження - особливості системи

Протягом багатьох років відеоспостереження є невід'ємною частиною комплексних систем безпеки. Воно застосовується при охороні промислових об'єктів, офісів, приватних будинків і навіть квартир. На відміну від своїх аналогових попередників, сучасне ip відеоспостереження дозволяє отримувати відмінну якість картинки за меншу ціну.

Як правило, до складу сучасної системи відеоспостереження входять такі компоненти:

- спеціалізований сервер або IP відеореєстратор;
- IP-відеокамери;
- PoE комутатор;
- кабельні системи[10].

Джерелами PoE є як комутатори з даною функціональністю, так і адаптери PoE. Адаптер підібрати досить просто, він повинен відповідати стандарту і класу, що підключається. А ось при виборі комутатора потрібно бути досить уважним. Так як до нього одночасно можуть підключатися пристрої різного класу і різних

стандартів 802.3af, 802.3at або 802.3bt. Потрібно звернути увагу на те які стандарти підтримує комутатор і яку потужність він може видати на спільні пристрої.

Потужність PoE комутатора можуть вказувати на кожен порт або сумарно максимальну потужність, яку комутатор може видати на всі порти, так званий «бюджет PoE».

- У першому випадку, PoE порти незалежні один від одного (в плані подачі живлення) і можуть видавати максимальну потужність на порт згідно підтримуваних стандартів. При підключенні пристроїв з малим споживанням надлишкова потужність не переноситися на сусідні порти.
- У разі комутаторів з бюджетом PoE, потужність ділиться між усіма портами PoE в залежності від класу підключеного пристрою. У разі якщо сумарна потужність підключених пристроїв перевищує бюджет PoE комутатора, на інші PoE порти живлення не подається. Найбільш поширені пристрої на сьогодні це комутатори з бюджетом PoE.

Не менш важлива складова частина всього вище сказаного це кабель. Він є середовищем передачі даних і живлення. Від якості кабелю залежить якість PoE і відстань на яке його можна провести. Мінімальна вимога - це чотири пари категорії 5e, з мідною жилою, опір провідника не повинно перевищувати 9,38 Ом на 100 метрів. При монтажі кабелю потрібно уникати сильних перегинів, а також потрібно правильно його заземлити.

Головною особливістю систем IP відеоспостереження є спосіб передачі відео даних. Сучасна система IP відеоспостереження передає зображення в цифровому форматі з допомогою мережі Ethernet.

Переваги систем IP відеоспостереження:

- В першу чергу варто відзначити якість картинки, яка відображається IP камерами. Сучасні пристрої даного типу здатні видавати відео зображення з роздільною здатністю 1080p і вище, що, в свою чергу, дозволяє розглянути дрібні деталі, такі як риси обличчя, елементи одягу, автомобільні номери, дрібні предмети та інше.

- Більшість IP камер мають вбудовану інфрачервону підсвітку, що дозволяє проводити зйомку в нічний час доби, а також внутрішній Micro SD порт. Слот для карт пам'яті дає можливість записувати і зберігати відео безпосередньо на відеокамері.
- Ще однією перевагою IP камер є можливість подачі електроживлення за допомогою технології PoE. Це означає, що напруга необхідна для роботи камери передається по тому ж проводу, що і картинка. Дане рішення дуже практичне і зручне. Також не варто забувати, що можна використовувати існуючу СКС при побудові системи IP відеоспостереження. Дані переваги суттєво спрощують установку системи, при цьому дозволяють заощадити значні фінансові кошти.
- Виробники пропонують провідні та безпровідні IP камери. Таке рішення дозволяє зробити їх установку навіть в самих важкодоступних місцях. При використанні бездротових камер відеоспостереження потрібно враховувати необхідність підведення електроживлення.
- Відеоспостереження IP, також, як і аналогове має в своєму складі відеореєстратор. На відміну від аналогового, цифровий реєстратор дозволяє зберігати відеоархів протягом тривалого періоду часу. Ще однією ключовою особливістю IP відеореєстратора є можливість його підключення до мережі Інтернет, завдяки чому перегляд картинки з камер може проводиться з будь-якої точки земної кулі.
- Устаткування для IP відеоспостереження невибагливе, просте в налаштуванні і використанні. Завдяки своїм перевагам, а також демократичній вартості, системи IP відеоспостереження користуються великою популярністю.

У разі прийняття рішення купити систему IP відеоспостереження ні в якому разі не варто прагнути заощадити. Купуючи дешеве обладнання низької якості можна отримати цілий ряд проблем, у вигляді поганої технічної підтримки, відсутність гарантії, невідповідності обладнання заявленим характеристикам і багато іншого.

Від якості та надійності системи відеоспостереження напряму залежить цілісність майна на об'єкті, що охороняється. З цієї причини ціна обладнання ні в якому разі не повинна відігравати ключову роль в процесі вибору і придбання системи безпеки.

Приклади обладнання зображені на Рисунках 3.13, 3.14, 3.15:


Рисунок 3.13 – IP-камера

Рисунок 3.14 – IP-відеореєстратор

Рисунок 3.15 – Комплект відеоспостереження

**Висновки до розділу**

1. Розглянуто структуру побудови систем управління та контролю доступу.

2. Проаналізовано технічні характеристики, на мою думку, найбільш вдалих рішень від охоронної системи Ajax. Описано широкі можливості пристроїв, з яких складається ця охоронна система.

3. Досліджено поєднання технологій передавання інформації, та технологій тривожного реагування.

# 4 ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Захист інформації в найширшому сенсі – це сукупність засобів захисту інформації від випадкового або навмисного впливу. Незалежно від того, що лежить в основі впливу: природні фактори або причини штучного характеру – власник системи несе збитки.

Забезпечення і підтримка інформаційної безпеки включає в себе комплекс різнопланових заходів, які запобігають, відстежують і усувають несанкціонований доступ третіх осіб. Заходи по захисту інформації спрямовані також на захист від пошкоджень, спотворень, блокування або копіювання інформації. Принципово потрібно, щоб всі завдання вирішувалися одночасно, тільки тоді забезпечується повноцінний, надійний захист.

Загрози інформаційної безпеки проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори вразливості. Загроза призводить до порушення діяльності систем на конкретному об'єкті.

Основні уразливості виникають унаслідок дії наступних факторів:

- недосконаліть програмного забезпечення, апаратної платформи;
- різні характеристики будови автоматизованих систем в інформаційному потоці;
- частина процесів функціонування систем є неповноцінною;
- неточність протоколів обміну інформацією та інтерфейсу;
- складні умови експлуатації інформації.

Найчастіше джерела загрози запускаються з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформації. Але можлива і випадкова дія загроз через недостатню міру захисту і масової дії фактору, що загрожує.

Існує поділ вразливостей за класами, вони можуть бути:

- об'єктивними;
- випадковими;
- суб'єктивними.

Якщо усунути або як мінімум послабити вплив вразливостей, можна уникнути повноцінної загрози, спрямованої на систему.

Кожна вразливість повинна бути врахована і оцінена фахівцями. Тому важливо визначити критерії оцінки небезпеки виникнення загрози і ймовірності поломки або обходу захисту інформації. Серед всіх критеріїв виділяють три основних:

- доступність - це критерій, який враховує, наскільки зручно джерелу загроз використовувати певний вид вразливості, щоб порушити інформаційну безпеку. У показник входять технічні дані носія інформації, на кшталт габаритів апаратури, її складності і вартості, а також можливості використання для злому інформаційних систем неспеціалізованих систем і пристроїв;
- фатальність - характеристика, яка оцінює глибину впливу вразливості на можливості фахівців впоратися з наслідками створеної загрози для інформаційних систем. Якщо оцінювати тільки об'єктивні вразливості, то визначається їх інформативність - здатність передати в інше місце корисний сигнал з конфіденційними даними без його деформації;
- кількість - характеристика підрахунку деталей системи зберігання та реалізації інформації, яким притаманний будь-який вид вразливості в системі.

Щоб дізнатися інформацію про ступінь захисту системи точно, потрібно залучати до роботи аналітичний відділ з експертами. Вони зроблять оцінку всіх вразливостей і складуть інформаційну. Результати всіх аналізів зводяться в одну таблицю, ступінь впливу розбивається по класах для зручності підрахунку коефіцієнта уразливості системи.

Не варто забувати про такі загрози, як випадкові і навмисні. Дослідження довели, що в системах дані регулярно піддаються різним реакціям на всіх стадіях циклу обробки і зберігання інформації, а також під час функціонування системи.

Як джерело випадкових реакцій виступають такі фактори, як:

- збої в роботі апаратури;

- періодичні шуми і фони в каналах зв'язку через вплив зовнішніх факторів, враховується пропускна здатність каналу, смуга пропускання;
- неточності в програмному забезпеченні;
- помилки в роботі співробітників або інших службовців в системі;
- специфіка функціонування середовища Ethernet;
- випадки під час стихійних лих або частих відключень електроживлення.

Похибки у функціонуванні програмного забезпечення зустрічаються найчастіше, а в результаті з'являється загроза. Всі програми розробляються людьми, тому не можна усунути людський фактор і помилки. Робочі станції, маршрутизатори, сервери побудовані на роботі людей. Чим вище складність програми, тим більше можливість розкриття в ній помилок і виявлення вразливостей, які призводять до загроз інформаційній безпеці.

Частина цих помилок призводить до небажаних результатів, наприклад, до відключення роботи сервера, несанкціонованого використання ресурсів, непрацездатності системи. Такі платформи, на яких була викрадена інформація, можуть стати майданчиком для подальших атак і представляють загрозу інформаційній безпеці.

Щоб забезпечити безпеку інформації в такому випадку, потрібно скористатися оновленнями. Встановити їх можна за допомогою паків, що випускаються розробниками. Встановлення несанкціонованих або неліцензійних програм може тільки погіршити ситуацію. Також можливі проблеми не тільки на рівні ПЗ, але і в цілому пов'язані з захистом безпеки інформації в мережі.

Якщо говорити про безпеку інтернету речей, то її можна скласти з наступних пунктів:

- безпека зв’язку;
- захист пристроїв;
- контроль пристроїв;

На цьому фундаменті можна створити потужну і просту в розгортанні систему безпеки, яка здатна послабити негативний вплив більшості загроз безпеки для інтернету речей, включаючи цілеспрямовані атаки. У цій статті ми описуємо

чотири фундаментальні напрямки, їх призначення і стратегії простої ефективної реалізації.

### 4.1 Безпека зв’язку

Канал зв'язку повинен бути захищений, для цього застосовуються технології шифрування і перевірки автентичності, щоб пристрої знали, чи можуть вони довіряти віддаленій системі. Нові криптографічні технології, такі як ECC (Elliptic Curve Cryptography), працюють в десять разів краще попередників. Не менш важливим завданням тут є управління ключами для перевірки достовірності даних та достовірності каналів їх отримання. Провідні центри сертифікації уже вбудували «сертифікати пристроїв» в більшість пристроїв IoT, надавши можливість виконувати перевірку автентичності широкого спектру пристроїв, включаючи стільникові базові станції, телевізори і багато іншого.

Шифрування, перевірка справжності і керованість є основою стійкої безпеки. Є чудові бібліотеки з відкритим вихідним кодом, які виконують шифрування навіть в пристроях IoT з обмеженими обчислювальними ресурсами. Але, на жаль, більшість компаній як і раніше піддаються небезпечним ризикам, допускаючи помилки при управлінні ключами для IoT.

Транзакції електронної торгівлі захищені простою і надійною моделлю довіри, яка обслуговує мільярди користувачів і понад мільйон компаній по всьому світу. Ця модель довіри допомагає системам безпечно проводити перевірку достовірності систем інших компаній і взаємодіяти з ними по зашифрованих каналах зв'язку. Модель довіри сьогодні є критичним фактором безпечної взаємодії в комп'ютерних середовищах і ґрунтується на дуже короткому списку довірених центрів сертифікації. Ці ж центри сертифікації встановлюють сертифікати в мільярди пристроїв щороку. Сертифікати пристроїв дозволяють, наприклад, перевіряти справжність мобільних телефонів для безпечного підключення до базових станцій, перевіряти справжність інтелектуальних лічильників для електроенергетики, а також приставок в індустрії кабельного телебачення. Надійні

центри сертифікації дозволяють легко і безпечно генерувати, видавати, реєструвати, контролювати і відкликати сертифікати, ключі та облікові дані, які мають вирішальне значення для надійної перевірки автентичності. З огляду на реалізовані обсяги сертифікатів безпеки для IoT, більшість сертифікатів пристроїв продаються великими партіями за невелику суму грошей за одиницю.

Перевірка справжності має значення. Небезпечно приймати дані від неперевірених пристроїв або неперевірених сервісів. Такі дані можуть пошкодити або скомпрометувати систему, передати контроль над обладнанням зловмисникам. Використання надійної перевірки автентичності для обмеження небажаних підключень допомагає вберегти системи IoT від подібних небезпек і зберегти контроль над вашими пристроями і сервісами. Незалежно від того, чи з'єднується пристрій з якимось іншим пристроєм або відбувається обмін даними з віддаленим сервісом, наприклад, хмарним, зв'язок завжди повинен бути захищеним. Всі взаємодії вимагають надійної перевірки автентичності і взаємної довіри. Виходячи з цих міркувань, економити на сертифікатах пристроїв не варто.

Більшість стандартів було розроблено для спрощення нам розгортання надійної перевірки автентичності всіх ланок ланцюга обміну даними. Стандарти існують для форматів сертифікатів, і надійні центри сертифікації підтримують як стандартні, так і створені по індивідуальному проекту формати. У більшості випадків сертифікатами можна легко керувати віддалено за допомогою стандартних протоколів, таких як Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) і Online Certificate Status Protocol (OCSP). Завдяки надійному центру сертифікації, який надає можливість обробляти сертифікати, ключі та облікові дані, фактичну перевірку справжності можна робити за допомогою потужних стандартів Transport Layer Security (TLS) і Datagram TLS (DTLS) – рідних SSL. Взаємна перевірка справжності, коли обидві кінцеві точки перевіряють один одного, має вирішальне значення для якісного захисту систем IoT. В якості додаткового бонусу, одного разу виконавши перевірку достовірності за TLS або DTLS, дві кінцеві точки можуть обмінюватися ключами шифрування або отримувати їх для обміну даними, які неможливо розшифрувати підслуховуючими

пристроями. Для багатьох додатків IoT потрібно абсолютна конфіденційність даних, це вимога легко виконується використанням сертифікатів і протоколів TLS/DTLS. Однак коли конфіденційність не є обов'язковою вимогою, справжність переданих даних може перевірятися будь-якою стороною, якщо вони були підписані під час їх появи на датчику - такий підхід не обтяжує канал шифруванням, що бажано в архітектурах multi-hop.

Часто виникають питання щодо вартості та продуктивності чіпів IoT для криптографічних операцій. Тут потрібно взяти до уваги, що Elliptic Curve Cryptography (ECC) в 10 разів швидше і ефективніше, ніж традиційне шифрування навіть в обмежених обчислювальними ресурсами пристроях. Така швидкість і ефективність досягаються без зниження рівня безпеки. ECC навіть продемонстрував рівень захисту, еквівалентний RSA 2048, в тому числі на надзвичайно обмежених в ресурсах чіпах - на 8-bit 1-MHz процесорах і 32-bit 1-KHz процесорах, при споживанні лише мікроват енергії. DTLS, варіант TLS був розроблений спеціально для малопотужних пристроїв, які періодично працюють між циклами сну. Ціна таких 32-розрядних чіпів незначна, тому ціну або потужність чіпів не вийде використовувати в якості аргументу для зниження вимог щодо захисту значень, які нижче розумних порогових, коли безпека має значення.

Сьогодні ми не можемо уявити собі таку незручність, як ручне встановлення сертифікатів в наші браузери для кожного веб-сервера, в той же час, ми не можемо уявити собі, яка це буде шкода, якщо сліпо вірити будь-якому сертифікату. Ось чому кожен браузер має кілька коренів довіри, за якими верифікуютсья всі сертифікати. Вбудовування цих коренів в браузери дало можливість масштабувати захист на мільйони серверів в Інтернеті. Оскільки мільярди пристроїв стають онлайн щорічно, в рівній мірі важливо, щоб в пристрої вбудовувалися і корні довіри, і сертифікат пристрою.

Дані, пов'язані з IoT, повинні зберігатися в безпеці весь час. Наше життя часто залежить від правильності, цілісності і належного функціонування цих систем більше, ніж від конфіденційності даних. Перевірка справжності інформації, пристроїв і походження інформації можуть мати вирішальне значення. Дані часто

зберігаються, кешуються і обробляються декількома вузлами, а не просто передаються з точки А в точку Б. З цих причин дані завжди повинні бути підписані в той момент, коли вони були вперше зафіксовані і збережені. Це допомагає знизити ризики будь-якого втручання в інформацію. Підписання об'єктів даних, як тільки вони були зафіксовані, і ретрансляція підпису з даними навіть після їх дешифрування є все більш поширеною і успішною практикою[4].

### 4.1.1 WPA2, WPA3

WPA2 (Wireless Protected Access ver. 2.0) – це друга версія набору алгоритмів і протоколів, які забезпечують захист даних в безпроводових мережах Wi-Fi. WPA2 суттєво підвищує захищеність безпроводових мереж Wi-Fi в порівнянні з колишніми технологіями. Новий стандарт передбачає, зокрема, обов'язкове використання більш потужного алгоритму шифрування AES (Advanced Encryption Standard) і аутентифікації 802.1x.

На сьогоднішній день для забезпечення надійного механізму безпеки в безпроводовій мережі необхідно використання пристроїв і програмного забезпечення з підтримкою засобів автентифікації та шифрування. Попередні покоління протоколів - WEP і WPA містять елементи з недостатньо сильними захистом і алгоритмами шифрування. Більш того, для злому мереж із захистом на основі WEP вже розроблені програми і методики, які можуть бути легко завантажені з мережі Інтернет і з успіхом використані навіть непідготовленими хакерами-новачками.

Протоколи WPA2 працюють в двох режимах автентифікації: персональному (Personal) і корпоративному (Enterprise). У режимі WPA2-Personal з введеної відкритим текстом парольної фрази генерується 256-розрядний ключ PSK (PreShared Key). Ключ PSK спільно з ідентифікатором SSID (Service Set Identifier) використовуються для генерації тимчасових сеансових ключів PTK (Pairwise Transient Key), для взаємодії безпроводових пристроїв. Як і статичному протоколу WEP, протоколу WPA2-Personal притаманні певні проблеми, пов'язані з

необхідністю розподілу і підтримки ключів на безпроводових пристроях мережі, що робить його більш відповідним для застосування в невеликих мережах з десятків пристроїв, в той час як для до корпоративних мереж оптимальний WPA2 - Enterprise.

У режимі WPA2-Enterprise вирішуються проблеми, що стосуються розподілу статичних ключів та управління ними, а його інтеграція з більшістю корпоративних сервісів автентифікації забезпечує контроль доступу на основі облікових записів. Для роботи в цьому режимі потрібні такі реєстраційні дані, як ім'я та пароль користувача, сертифікат безпеки або одноразовий пароль, автентифікація ж здійснюється між робочою станцією і центральним сервером автентифікації. Точка доступу або безпроводовий контролер проводять моніторинг підключень і направляють автентифікаційні запити на відповідний сервер автентифікації. Базою для режиму WPA2-Enterprise служить стандарт 802.1x, що підтримує автентифікацію користувачів і пристроїв, придатну як для проводових комутаторів, так і для безпроводових точок доступу[8].

Advanced Encryption Standard (AES) - симетричний алгоритм блочного шифрування, прийнятий урядом США як стандарт в результаті конкурсу, проведеного між технологічними інститутами.

Цей алгоритм, крім абревіатури AES, іноді називають ще Rijndael - це анаграма з частин імен бельгійських програмістів Joan Daemen і Vinent Rijmen, які розробили AES. Строго кажучи, AES і Rijndael - не зовсім одне й те саме, оскільки AES має фіксований розмір блоку в 128 біт і розміри ключів в 128, 192 і 256 біт, в той час як для Rijndael можуть бути задані будь-які розміри блоку і ключа, від мінімуму в 32 біт до максимуму в 256 біт.

Вважається, що ключ, який використовується в Advanced Encryption Standard, довжиною в 128 біт – досить надійний захист проти лобової атаки, тобто з суто математичної точки зору підібрати один правильний пароль з усіх можливих є доволі важким завданням. Незважаючи навіть на деякі недоліки AES, зламати захищену за допомогою цього алгоритму інформацію практично нереально.

Довжина ключа, що використовується при шифруванні і визначає практичну

доцільність виконання повного перебору, адже інформацію зашифровану довшими ключами експоненціально складніше зламати, ніж з короткими.

Основна ідея впровадження нового протоколу WPA3 - усунення концептуальних недоліків протоколу WPA2, і зокрема, захист від атак з перевстановленням ключа. Протокол WPA3 володіє більш високим рівнем безпеки, в порівнянні з WPA2. WPA3 також передбачає в собі два режими роботи WPA3-Personal і WPA3-Enterprise. WPA3-Personal (WPA3-PSK) забезпечує 128-бітове шифрування даних, а WPA3-Enterprise 192-бітове.

У WPA2 постійною проблемою залишалося використання слабких паролів. Якщо користувачі ставлять легкий пароль на безпроводову мережу, то його без зусиль можна було підібрати за допомогою автоматизованих атак з використанням словників, таких як Dictionary і Brute-Force. Протокол WPA2 ніколи не пропонував варіантів для вирішення цієї проблеми. Від розробників були лише рекомендації використовувати складні і більш надійні паролі. У WPA3 вжиті заходи, що дозволяють протидіяти таким атакам.

Для цього в WPA3 був реалізований новий механізм автентифікації SAE (Simultaneous Authentication of Equals), який замінює використовуваний в WPA2 метод PSK (Pre-Shared Key). Саме в PSK описано чотириступінчасте рукостискання для встановлення зв'язку. Цей метод був скомпрометований KRACK-атакою, яка перериває серію рукостискань і намагається повторити запит на підключення. Неодноразова повторна відправка повідомлень змушує учасників мережі перевстановити узгоджений ключ. Коли жертва переустановлює ключ, асоційовані з ним параметри скидаються, що порушує безпеку, яку повинен гарантувати WPA2. Таким чином, зловмисник отримує можливість прослуховувати трафік і розповсюджувати свої пакети.

SAE перекладається як "одночасна автентифікація рівних", і як зрозуміло з назви, згідно з цим алгоритмом автентифікація пристроїв проводиться одночасно і на рівних правах.

Розробники відмовилися від суворої послідовності дій при авторизації і пішли від того, щоб вважати точку доступу головним пристроєм в мережі при

авторизації. Згідно з механізмом SAE, всі пристрої в мережі працюють на рівних правах. Тому будь-який пристрій може почати відправляти запити на автентифікацію і в довільному порядку відправляти інформацію по встановленню ключів. В результаті чого, можливість реалізації KRACK-атаки була усунена. З появою SAE у зловмисника принципово не буде можливості перервати процес автентифікації, влізаючи між точкою доступу і абонентським пристроєм[9].

WPA3 усуває слабкість і забезпечує набагато більшу безпеку. Наприклад, WPA3-Personal забезпечує шифрування для користувачів, навіть якщо хакери зламають ваш пароль після підключення до мережі.

128-бітний AES залишається на місці для WPA3. Однак для з'єднань WPA3-Enterprise потрібен 198-бітний AES. Користувачі WPA3-Personal також матимуть можливість використовувати надміцний 198-бітний AES.

### 4.2 Захист пристроїв

Захист пристроїв – це в першу чергу забезпечення безпеки і цілісності програмного коду. Підписання коду потрібно для підтвердження правомірності його запуску, також необхідний захист під час виконання коду, щоб атаки не перезаписали його під час завантаження. Підписання коду криптографічно гарантує, що він не був зламаний після підписання і безпечний для пристрою. Це може бути реалізовано на рівнях Application і Firmware і навіть на пристроях з монолітним чином прошивки. Всі критично важливі пристрої, датчики, контролери або щось ще, повинні бути налаштовані на запуск тільки підписаного коду.

Пристрої повинні бути захищені і на наступних етапах, вже після запуску коду. Тут допоможе захист на основі хоста, розмежування доступу до системних ресурсів і файлів, контроль підключень, захист від вторгнень, захист на основі поведінки і репутації. Також в цей довгий список можливостей хостового захисту входять блокування, протоколювання і оповіщення для різних операційних систем IoT. Останнім часом багато засобів хостового захисту були адаптовані для IoT і тепер добре опрацьовані і налагоджені, не вимагають доступу до хмари і дбайливо

витрачають обчислювальні ресурси IoT-пристроїв.

У попередньому розділі ми розглянули перший аспект захисту пристроїв, який визначає основні принципи управління ключами, перевірки автентичності для IoT, підписання коду і конфігурації для захисту цілісності пристрою, основи управління таким кодом і конфігурацією. Однак, після захисту зв'язку і реалізації безпечного завантаження добре керованого пристрою, необхідний захист на етапі експлуатації. Хостовий захист вирішує цю задачу.

IoT-пристрої стикаються з багатьма загрозами, в тому числі шкідливим кодом, який може поширюватися через перевірені з'єднання, скориставшись вразливостями або помилками в конфігурації. В таких атаках часто експлуатуються кілька слабких місць, включаючи, невикористання перевірки підпису коду і безпечне завантаження, а також погано реалізовані моделі перевірки, які можна обійти.

Атакуючі часто використовують ці недоліки для витягання конфіденційної інформації з системи, а іноді навіть для інфраструктури Command&Control (C&C) для маніпулювання поведінкою системи. Особливо тривожить здатність деяких зловмисників експлуатувати вразливості для установки шкідливих програм прямо в пам'ять вже працюючих систем IoT. Причому іноді вибирається такий спосіб зараження, при якому шкідлива програма зникає після перезавантаження пристрою, але встигає наносити величезної шкоди. Це працює, тому що деякі системи IoT і багато промислових систем майже ніколи не перезавантажуються. Для відділу безпеки в цьому випадку ускладнюється можливість виявлення використаної уразливості в системі і розслідування походження атаки. Іноді такі атаки відбуваються через IT-мережу, підключену до промислової мережі або до мережі IoT, в інших випадках атака відбувається через інтернет або через прямий фізичний доступ до пристрою. Таким чином, безпека IoT повинна бути комплексною.

В поєднанні з надійним підписом коду і моделлю перевірки, хостовий захист може допомогти захистити пристрій від безлічі небезпек. У хостового захисту використовується ряд технологій захисту, в тому числі харденінг, розмежування

доступу до системних ресурсів, захист на основі репутації і поведінки, захист від шкідливих програм і, нарешті, шифрування. Залежно від потреб конкретної системи IoT комбінація цих технологій може забезпечити найвищий рівень захисту для кожного пристрою.

Харденінг, розмежування доступу до ресурсів захистять всі входи в систему. Вони обмежують мережеві підключення до додатків і регламентують вхідний і вихідний потік трафіку, захищають від різних експлойтів, переповнення буфера, цілеспрямованих атак, регулюють поведінку додатків, при цьому дозволяють зберегти контроль над пристроєм. Такі рішення ще можуть використовуватися для запобігання несанкціонованого використання знімних носіїв, блокування конфігурації та налаштувань пристрою і навіть для деескалації користувальницьких привілеїв, якщо потрібно. Хостовий захист має можливості аудиту і оповіщення, допомагаючи відстежувати журнали і події безпеки. Технології на основі політик можуть працювати навіть в середовищах без підключення до інформаційної мережі або при обмеженій обчислювальній потужності, необхідної для використання традиційних технологій.

Технологія захисту на основі репутації може використовуватися для визначення сутності файлів по їхньому віку, поширеності, розташування і до решти для виявлення небезпек, що не виявляються іншими засобами, а також давати уявлення про те, чи слід довіряти новому пристрою навіть при успішній перевірці автентичності. Таким способом можна ідентифікувати загрози, які використовують мутуючий код або адаптують свою схему шифрування, просто відокремлюючи файли з високим ризиком від безпечних, швидко і точно виявляючи шкідливі програми, незважаючи на всі їхні хитрощі.

Зрозуміло, що поєднання застосовуваних технологій буде залежати від конкретної ситуації, але наведені вище засоби можуть об'єднуватися для захисту пристроїв, навіть в середовищах з обмеженими обчислювальними ресурсами.

### 4.3 Контроль пристроїв

Управління безпекою кожного пристрою може припускати управління конфігурацією за допомогою хостового захисту, який ми розглянули в попередньому розділі. Також існують технології безпеки, засновані на політиках, яким поновлення потрібні тільки при перевстановленні на пристрої програмного забезпечення для якихось цілей, наприклад, для додавання функціональних можливостей. Проте обидва типи технологій можуть генерувати телеметрію безпеки, яка має велике значення при зіткненні з цілеспрямованими атаками. Тому телеметричні дані безпеки завжди повинні збиратися від цих технологій для централізованого аналізу.

Компоненти безпеки не єдині в пристрої IoT, якими необхідно управляти безпечно і надійно. Більшість пристроїв генерують телеметрію або дані з датчиків, які потрібно також безпечно і надійно збирати і передавати в місця зберігання та аналізу. Багато пристроїв вже містять в собі функції контролю, якими потрібно акуратно управляти через конфігураційні параметри, а ті в свою чергу безпечно і надійно зберігати і оновлювати. На щастя, інфраструктури управління пристроями, які використовують загальноприйняті безпечні протоколи, можуть застосовуватися і для захищеного управління основними функціями пристрою, контентом безпеки і телеметрії пристрою. Деякі з інфраструктур управління комбінують агентські та безагентські протоколи управління IoT, тоді як пристрої випускаються з підтримкою стандартизованого управління для спрощення функцій контролю. А окремі інфраструктури управління можуть додатково поєднувати всі ці методи управління з розумінням інформації, отриманої від мережевих аналізаторів трафіку.

В такій ситуації системи IoT повинні спочатку мати вбудовані можливості оновлення OTA. Відсутність цих можливостей залишить пристрої піддатливими до загроз і вразливостей протягом всього терміну їх служби. Зрозуміло, оновлення OTA може застосовуватися ще для управління конфігураціями пристроїв, контентом безпеки, обліковими даними, а також для розширення функціональних можливостей пристроїв, збору телеметрії і даних програмного оточення, для

доставки патчів безпеки і багато чого іншого. Однак з додатковою функціональністю або без неї базові можливості поновлення і управління захищеністю повинні бути передбачені ще на етапі проектування пристроїв IoT[5].

**Висновки до розділу**

1. Системи IoT бувають дуже складними, їм потрібні комплексні заходи захисту, також необхідна підтримка пристроїв IoT з обмеженими обчислювальними ресурсами, яких недостатньо для підтримки традиційних рішень безпеки. Простого універсального рішення не існує. Безпека повинна бути всебічною, інакше атакуючі просто скористаються найслабшою ланкою. Звичайно, традиційні IT-системи як правило передають і обробляють дані з систем IoT, але самі системи IoT володіють своїми унікальними потребами в захисті.

2. Архітектура зниження впливу шкідливого коду гарантує, що весь код криптографічно підписаний і авторизований для пристрою, непідписаний код не дозволений для запуску.

Захищений зв'язок за допомогою взаємної перевірки автентичності та шифрування. Застосовуються перевірені часом центри сертифікації і моделі довіри, які вже захищають більшість IoT-пристроїв. Використовуються нові алгоритми ECC для забезпечення високого рівня безпеки в пристроях IoT з обмеженими обчислювальними ресурсами.

Ця архітектура додатково послаблює шкідливу дію за допомогою хостового захисту і підсилює ефективність мінімізацією ризиків від всіх інших загроз за допомогою аналітики безпеки.

При виявленні вразливостей і загроз ризик їх реалізації можна знизити за допомогою ефективного, надійного і захищеного динамічного управління системою.

Залишається лише додати, що успішне забезпечення безпеки систем починається з моделювання ризиків. Без розуміння, як зловмисники можуть скомпрометувати систему, малоймовірно надійно захистити будь-яку систему.

# 5 СТАРТАП-ПРОЕКТ

## 5.1 Основні відомості

Сутність стартап-проекту. Досліджуючи ринок Інтернету речей було виявлено можливість вдосконалення систем безпеки, охоронних систем та систем обмеження доступу, які впроваджуються щодня все з більшими темпами та в більших масштабах. Зміст ідеї стартапу та визначення її характеристик наведено в табл. 5.1 та табл. 5.2.

Таблиця 5.1 – Зміст ідеї стартап-проекту

| Зміст ідеї | Напрямки застосування | Вигоди для користувача |
|---|---|---|
| Запропонувати ефективні рішення рішення для підви-щеня надійності та забезпечення безпеки в системах забезпечення безпеки в умовах різних проектів. | Охоронні системи та системи обмеження доступу | Надійний зовнішній зв’язок та зв’язок між пристроями системи, а значить і високий рівень безпеки |

Таблиця 5.2 – Визначення характеристик ідеї стартап-проекту

| № п/п | Техніко-економічні характеристики ідеї | (потенційні) товари/концепції конкурентів | | W (слабка сторона) | N (нейтральна сторона) | S (сильна сторона) |
|---|---|---|---|---|---|---|
| | | Запропонований метод | Загальновживаний метод | | | |
| 1. | Поєднання різних видів захисту в залежності від вимог замовника | Дає змогу | Дає змогу | Залежить від випадків застосування | Кінцевий споживач може бути незадоволений ціновою політикою | Легкість у використанні, широка інтегрованість |
| 2. | Висока надійність, завдяки поєднанню технологій | Дає змогу | Не дає змогу | Додаткова плата за використання каналів зв'язку | Постійна підтримка та розробка оновлень які будуть запобігати новим вразливостям | Простота та зручність налаштувань |

## 5.2 Технологічний аудит ідеї стартап-проекту

В таблиці 5.3 оцінено можливість технологічної реалізації ідеї стартапу та показано технології, які можна застосувати для реалізації проекту.

Таблиця 5.3. Технологічна здійсненність ідеї проекту

| № п/п | Ідея проекту | Технології її реалізації | Наявність технологій | Доступність технологій |
|---|---|---|---|---|
| 1 | Інтеграція рішень забезпечення безпеки для покращення надійності охоронних систем в рамках різних проектів та компаній | Обладнання, яке підтримує поєднання технологій зовнішнього зв’язку | Присутня | Доступна в випадку достатнього бюджету |
| 2 | | Використання технологій для внутрішнього обміну інформацією | Присутня | Доступна в випадку достатнього бюджету |
| 3 | | Програмні рішення на всіх пристроях системи | Необхідно розробити | Доступна в випадку достатнього бюджету |

Обрана технологія реалізації ідеї проекту: застосування комплексу рішень та технологій для покращення надійності охоронних систем та підвищення рівня безпеки.

## 5.3 Аналіз можливостей ринку для запуску проекту

У таблиці 5.4 показано попередню характеристику потенційного ринку стартап-проекту.

Таблиця 5.4. Попередня характеристика потенційного ринку стартапу

| № п/п | Показники ринку (найменування) | Характеристика |
|---|---|---|
| 1 | Кількість основних гравців, од | 3 |
| 2 | Обсяг продажів, грн/ум.од | 900000 |
| 3 | Тенденції ринку (якісна оцінка) | Швидко зростає |
| 4 | Обмеження для входу (вказати характер обмежень) | Пошук потенційних клієнтів |
| 5 | Специфічні вимоги стандартизування та сертифікування | Ліцензія на діяльність, сертифікація співробітників в галузі мережевих технологій |
| 6 | Середня норма рентабельності в даній галузі, % | 900000/610000 = 148% |

У таблиці 5.5 показано характеристику потенційних клієнтів стартап-проекту

Таблиця 5.5. Характеристика потенційних клієнтів стартап-проекту

| № п/п | Потреба, що формує ринок | Цільова аудиторія (цільові сегменти ринку) | Відмінності поведінки потенційних цільових груп клієнтів | Вимоги споживачів до товару |
|---|---|---|---|---|
| 1 | Забезпечення безпеки власного майна | Звичайні громадяни | Забезпечення зростання якості життя населення | Результат повинен відповідати найвищим стандартам якості безпеки актуальним відповідним загрозам та вразливостям які змінюються з кожним днем |

Продовження табл. 5.5

| | | | | |
|---|---|---|---|---|
| 2 | Необхідність застосування систем контролю та управління доступом | Компанії, які працюють з персональними даними та іншими джерелами цінної інформації | Кожна група має компаній має власні вимоги до технічного забезпечення та політик і засобів безпеки відповідно | Забезпечення безпеки в залежності від потреб споживача |

У табл. 5.6 наведено основні загрози реалізації стартап-проекту.

Таблиця 5.6. Фактори загроз

| № п/п | Фактор | Опис загрози | Планове реагування компанії |
|---|---|---|---|
| 1 | Конкуренція | Велика кількість пристроїв та засобів безпеки на сьогодні | Реалізація послуг на найвищому рівні для надання максимально можливих та гнучких послуг відповідно до потреби клієнта |
| 2 | Швидка зміна ринку та технологій | Складність відповідати тенденціям ринку безпеки для надання актуальних послуг | Інвестиції в сертифікацію, моніторинг сучасних рішень, які враховують потреби так званого «завтрашнього дня» |

У табл.5.7 наведено основні можливості під час реалізації стартап-проекту.

Таблиця 5.7. Основні можливості

| № п/п | Фактор | Опис можливості | Планове реагування компанії |
|---|---|---|---|
| 1 | Лідерські позиції на ринку інтеграції рішень безпеки | Стрімке зростання попиту та кількісне зростання систем безпеки | Якісне та кількісне збільшення потужностей |
| 2 | Впровадження запропонованих технологій в уже існуючі системи забезпечення безпеки | Збільшення об'ємів закупівель та пошук технологічних рішень для ширшого охоплення ринку | Якісне та кількісне збільшення потужностей |

У таблиці 5.8 наведено особливості та вплив конкурентного середовища на впровадження проекту.

Таблиця 5.8. Аналіз конкуренції

| Особливості конкурентного середовища | Прояв даної характеристика | Вплив на діяльність підприємства (планові дії компанії для забезпечення конкурентоспроможності) |
|---|---|---|
| 1.Конкуренція | Застосування вже існуючих технологій | Проведення стандартизації на високому рівні |
| 2.Локальний | Відсутність єдиного постачальника послуг | Індивідуальний підхід до кожної локальної ділянки |
| 3.Міжгалузева | Відсутня | Відсутня |
| 4.Товарно-видова | Використання стандартизованих технологій | Застосування загальновживаних апаратних та програмних засобів, за необхідності |
| 5.Цінова | Використання високовартісних спеціалізованих комплексів | Використання гнучких універсальних програмних засобів для компенсації апаратної частини |
| 6.Марочна | Кожна діагностика повинна бути стандартизованою | Здобуття лідерських позицій на ринку інтеграції рішень безпеки |

У таблиці 5.9 проаналізовано конкуренцію проекта в галузі за М. Портером

Таблиця 5.9. Аналіз конкуренції за М. Портером

| Складові аналізу | Прямі конкуренти | Потенційні конкуренти | Постачальники | Клієнти | Товари-замінники |
|---|---|---|---|---|---|
| | Системні інтегратори | Нові гравці ринку систем безпеки | Залучення лише провідних в цій галузі постачальників | Самостійність у прийнятті клієнтських рішень | Надання переваги компаніям які займають лідерські позиції та мають репутацію інноваційних та технологічних протягом всього часу існування на ринку |
| Висновки: | Середня | Є можливість виходу на ринок | Постачальники встановлюють цінову політику на обладнання | Клієнти встановлюють вимоги до якості | Обмеженнь немає |

У табл. 5.10 наведено та обґрунтувано фактори конкурентноспроможності.

Таблиця 5.10. Обґрунтування факторів конкурентоспроможності

| № п/п | Фактор конкурентоспроможності | Обґрунтування (чинники, що роблять фактор порівняння конкурентних проектів значущим) |
|---|---|---|
| 1 | Раціональніша цінова політика | Можливість раціональнішого використання ресурсів |
| 2 | Забезпечення сервісних послуг | Сервісне обслуговування програмної та апаратної частини |

У табл. 5.11 перелічено сильні та слабкі сторони проекту.

Таблиця 5.11. Порівняльний аналіз сильних та слабких сторін проекту

| № п/п | Фактор конкурентоспроможності | Бали 1-20 | Порівняння рейтингу товарів-конкурентів | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | –3 | –2 | –1 | 0 | +1 | +2 | +3 |
| 1 | Раціональніша цінова політика | 13 | | | + | | | | |
| 2 | Послуги сервісного обслуговування | 16 | | | + | | + | | |
| 3 | Періодична діагностика | 10 | | | | | + | | |
| 4 | Потреба в залученні висококваліфікованих кадрів | 15 | | | | | | + | |

У табл.5.12 представлений SWOT-аналіз стартап-проекту.

Таблиця 5.12. SWOT- аналіз стартап-проекту

| | |
|---|---|
| Сильні сторони: раціональна цінова політика, постачання апаратного та програмного забезпечення | Слабкі сторони: потреба в залученні висококваліфікованих кадрів, постійна перепідготовка та актуалізація знань, стеків протоколів та програмних і апаратних засобів |
| Можливості: Інноваційна технологічно-економічна модель інтеграції рішень забезпечення безпеки для реалізації на різних рівнях охоронних систем | Загрози: Конкуренція на швидко зростаючому та ринку, його збільшення, нові гравці та технології |

Альтернативи ринкового впровадження стартапу показані в табл.5.13.

Таблиця 5.13. Альтернативи ринкового впровадження роекту

| № п/п | Альтернатива (орієнтовний комплекс заходів) ринкової поведінки | Ймовірність залучення ресурсів | Терміни реалізації |
|---|---|---|---|
| 1 | Складання договорів з технічними компаніями для інтеграції та постачання на ексклюзивних правах в залежності від обсягів замовлення для подавлення конкурентів замовником за рахунок реалізованих системних рішень | висока | короткі |
| 2 | Застосування інноваційних технологій та комплексів систем і програмного забезпечення для швидкого зростання на ринку | висока | короткі |

## 5.4. Розроблення ринкової стратегії проекту

Обгрунтування вибору цільових груп потенціійних споживачів показано в табл. 5.14 [31].

Таблиця 5.14. Вибір цільових груп потенційних споживачів

| № п/п | Загальний профіль цільової групи потенційних клієнтів | Готовність сприйняття продукту споживачами | Орієнтовний попит цільової групи (сегменту) | Напруженість конкуренції в сегменті | Складність входу у сегмент |
|---|---|---|---|---|---|
| 1 | Звичайні громадяни | Висока | Високий | Середня | Середня |
| 2 | Системи Інтернету речей в різних галузях та напрямках які на сьогодні широко розповсюджені | Середня | Середній | Середня | Низька |

Визначення базової стратегії розвитку наведено у табл. 5.15.

Таблиця 5.15. Визначення базової стратегії розвитку

| № п/п | Обрана альтернатива розвитку проекту | Стратегія охоплення ринку | Основні конкурентоспроможні позиції згідно з обраною альтернативою | Базова стратегія розвитку* |
|---|---|---|---|---|
| 1 | Застосування альтернативних технологій та пристроїв | Впровадження нового стандарту якості | Залучення ключових гравців у галузі | Стратегія диференціації |
| 2 | Бюджетність проекту в порівнянні з іншими гравцями ринку | Інвестиція в кваліфіковані кадри | Використання унікальних, інноваційних, передових рішень для досягнення лідерських позицій | Стратегія лідерства по якості послуг та рівню обслуговування |

Визначення основної стратегії конкурентної поведінки показано в табл. 5.16.

Таблиця 5.16. Визначення базової стратегії конкурентної поведінки

| № п/п | Чи є проект унікальним на ринку? | Чи необхідно буде компанії шукати нових споживачів, чи опрацьовувати існуючих у конкурентів? | Чи необхідно компанії копіювати основні характеристики товару конкурента? | Стратегія конкурентної поведінки* |
|---|---|---|---|---|
| 1 | Ні | Опрацьовувати існуючих та шукати нових | Немає необхідності | Стратегія інноваційної конкуренції |

Визначення стратегії позиціонування показано в табл. 5.17.

Таблиця 5.17. Визначення стратегії позиціонування

| № п/п | Вимоги цільової аудиторії до товару | Основна стратегія розвитку | Основні конкурентоспроможні позиції стартап-проекту | Визначення асоціацій, які сформують комплексну позицію стартап-проекту (три основних) |
|---|---|---|---|---|
| 1 | Належна висока якість послуг | Стратегія диференціації | Новизна, гарант якості, точність дослідження | Якість, точність, надійність |
| 2 | Раціональні витрати | Стратегія лідерства по витратах | Гнучкість запропонованого рішення | Універсальність, інноваційність, надійність |

## 5.5. Розроблення маркетингової програми стартап-проекту

Основні переваги концепції потенційного товару показано в табл. 5.18.

Таблиця 5.18. Визначення основних переваг концепції потенційного товару

| № п/п | Потреба | Вигода, яку пропонує товар | Основні переваги перед конкурентами (існуючі або потенційні) |
|---|---|---|---|
| 1 | Якість | Належна висока якість, надійність | Масштабованість, гнучкість, якість |
| 2 | Раціональна вартість | Оптимальне використання коштів, максимальна якість обладнання від провідних постачальників, максимальний рівень кваліфікації спеціалістів в залежності від вартості та складності проекту | Раціоналізація витрат відповідно до розміру бюджету замовника |

Виявлено три рівні моделі товару. Зміст та складові рівнів товару показано в табл. 5.19.

Таблиця 5.19. Опис трьох рівнів моделі товару

| Рівні товару | Зміст та складові | | |
|---|---|---|---|
| I. Товар за задумом | Якісний товар та послуги, стандартизована якість послуг та обладнання | | |
| II. Товар у реальному виконанні | Властивості/характеристики | М/Нм | Вр/Тх /Тл/Е/Ор |
| | 1)Вартість обслуговування,<br>2)Кількість комплектів обладнання<br>3)Строк безвідмовної експлуатації<br>4)Технологічна собівартість товару | 1) М<br>2) М<br>3) М<br>4) М | 1)Е<br>2) Пр<br>3)Нд<br>4)Тх |
| | Якість: міжнародні стандарти, постійне обслуговування та підтримка обладнання | | |
| | Постачання, розрахунки та інтеграція під конкретні системи | | |
| | Марка: Системи безпеки | | |
| III. Товар із підкріпленням | До продажу – обладнання та встановлення | | |
| | Після продажу – аудит та вдосконалення застарілих елементів та систем в цілому в залежності від актуальних вимог та потреб | | |

Потенційний товар буде захищено від копіювання завдяки: товарна марка та унікальні рішення, які не мають аналогів на ринку та відрізняються між собою оскільки кожне з рішень є глибоко індивідуальним в залежності від потреб замовника, що необхідно для забезпечення найвищих та актуальних на майбутнє стандартів безпеки.

Визначення цінової політики на послугу показано в табл. 5.20.

Таблиця 5.20. Визначення меж встановлення ціни

| № п/п | Цінова політика товарів-замінників | Цінова політика на товари-аналоги | Рівень купівельної спроможності цільової групи споживачів | Верхня та нижня межі встановлення ціни на товар/послугу |
|---|---|---|---|---|
| 1 | 30000 у.о./од. (стандартні системи безпеки) | - | Дуже високий | Н.1000 у.о. – В.100000 у.о. (Товар)<br>Н.1000 у.о. – В.100000 у.о. (Послуга) |

Створення системи збуту послуги вказано у табл. 5.21.

Таблиця 5.21. Створення системи збуту

| № п/п | Закупівельна поведінка цільових клієнтів | Функції збуту, що повинен забезпечувати постачальник товару | Глибина каналу збуту | Оптимальна система збуту |
|---|---|---|---|---|
| 1 | Орієнтована на максимальний рівень в системах безпеки | Поставки якісного обладнання та інноваційних рішень | Значна | Контрактна система |

Концепції маркетингових комунікацій показано в табл. 5.22.

Таблиця 5.22. Концепція маркетингових комунікацій

| № п/п | Специфіка поведінки цільових клієнтів | Канали комунікацій цільових клієнтів | Основні методи позиціонування | Завдання рекламного звернення | Концепція рекламного звернення |
|---|---|---|---|---|---|
| 1 | Зацікавленість якісному та якісному продукті з раціональним використанням ресурсів | Мережеві ресурси | Гарантія якості та стандартизація, сервісна політика | Привернути увагу до покращень, пов’язаних із зростаючою потребою в захисті | Позиціонування безпеки як основи для побудови надійних рішень та іміджу компанії |
| 2 | Зацікавленість у великих об’ємах продукції із дотриманням умов якості | Мережні ресурси | Глибина каналу постачальників, гарант якості | Привернути увагу до переваг над іншими гравцями ринку | Позиціонування як активного та інноваційного гравця ринку на фоні конкурентів |

**Висновки до розділу**

1. Виявлено, що комерціалізацію стартап-проекту щодо застосування та розвитку комплексу апаратних та програмних рішень для забезпечення безпеки в охоронних системах та системах обмеження доступу можна вважати доцільною та актуальною в умовах надшвидкого розвитку галузі. На ринку технічних рішень попит на дану пропизицію все більше зростає, який зараз задовольняють товари замінники та більш вузьконаправлені рішення, саме тому необхідно виходити на ринок та пропонувати широкий спектр рішень для забезпечення потреб ринку та розвитку спектру послуг. Рентабельність на ринку забезпечить в першу чергу можливість заміни існуючих рішень на більш масштабовані, гнучкі та інноваційні, шляхом застосування комплексних рішень.

2. Перспективність впровадження досить висока, адже основними клієнтами є звичайні громадяни а також компанії, які активно впроваджують охоронні системи та системи контролю та управління доступом. Конкурентноспроможність проекту забезпечує високий рівень кваліфікації у підході до вирішення та реалізації кожного конкретного рішення та звернення зі сторони клієнта, максимальна гнучкість у плані рівня реалізованих систем в залежності від типу, бюджету клієнта та особливостей застосування.

3. Обрана альтернатива впровадження – пошук актуальних та інноваційних рішень, їх поширення та популяризація в умовах ринку. Імплементація проекту доцільна, а сприятливі умови для його розвитку обумовлені рентабельністю та зацікавленістю потенційних груп компаній та окремих клієнтів.

# ВИСНОВКИ

У магістерській дисертації досліджено можливість вирішення проблеми підвищення надійності системи забезпечення безпеки в процесі інтеграції різних технологій, що забезпечать гнучкість, масштабованість та технологічність таких рішень в умовах стрімкого розвитку технологій Інтернету речей та відповідно нових загроз та вразливостей.

1. Проаналізувавши, основні види загроз та вразливостей, які існують на сьогодні, наслідки яких можуть бути спричинені як для звичайних громадян так і для підприємств та компаній, до основних загроз віднесено несанкціонований доступ, перехоплення управління, виникнення пожежі, аварії та інших небезпечних для життя і здоров’я людей ситуації.

2. Обґрунтовано, що для реалізації охоронних систем доцільно надавати перевагу технології Jeweller. Технологія забезпечує двосторонній тип та досить великий радіус зв’язку, має блочне шифрування, максимальна кількість пристроїв, що можуть підключитись досягає 100 одиниць, має захист від глушіння.

3. При розгляді структури охоронної системи надав перевагу пристроям безпроводової системи Ajax. Технологія обрана в попередньому розділі була розроблена під цю систему. Система має ряд переваг перед іншими, віддалене налаштування, для зв’язку з кожним пристроєм централь використовує вільну частоту і перебудовується на іншу в разі збігу, а також доволі довгий термін роботи датчиків. Цей термін при щохвилинних пінгах може становити до 7 років. Також в системі присутній модуль GSM, який надає резервний канал зв’язку в разі відключення інтернету.

4. Для забезпечення захисту інформації в системах Інтернету речей слід приділити увагу таким аспектам як безпека зв’язку, захист та контроль пристроїв. Захист пристроїв – це в першу чергу забезпечення безпеки і цілісності програмного коду. Підписання коду криптографічно гарантує, що він не був зламаний після підписання і безпечний для пристрою. Для безпеки зв’язку використовуються технології шифрування та перевірки автентичності. Для проведення автентифікації

пропонується обрати набір алгоритмів та протоколів WPA2 або WPA3. Щодо методу шифрування слід надати перевагу симетричному алгоритму блочного шифрування Advanced Encryption Standard (AES).

5. Розроблено стартап-проект, який базується на просуванні на ринок Інтернету речей рішень на базі охоронних систем як комплексного рішення для інтеграції в системи забезпечення безпеки. Проведено дослідження доцільності та рентабельності даного бізнес-проекту та визначено, що комерціалізація проекту є доцільною.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Класифікація загроз: В.А. Ворона, В.А. Тихонов «Системы контроля и управления доступом»

2. СКУД – ключові тренди // Олексій Гінце – Специальный выпуск журнала «Системы безопасности», 2018

3. Як смартфон витісняє карти з ринку СКУД // Лоза А. – Специальный выпуск журнала «Системы безопасности», 2018

4. Захист інформації в системах IoT, опис безпеки зв'язку. URL: https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1

5. Захист інформації в системах IoT, опис захисту та безпеки пристроїв. URL: https://www.anti-malware.ru/practice/solutions/iot-reference-architecture-protection-part-2

6. Опис технології LoRaWAN. URL: https://deps.ua/knowegable-base-ru/spravochnaya-informatsiya/item/66633.html

7. Огляд технологій Інтернету речей. URL: http://ua.automation.com/content/wifi-bluetooth-ili-zigbee-kakoj-standart-luchshe

8. Огляд WPA2. URL: https://okdk.ru/wep-protiv-wpa-protiv-wpa2-protiv-wpa3-obyasneniya-tipov-bezopasnosti-wi-fi/

9. Новий протокол для WPA3. URL: https://www.depo.ua/rus/life/wi-fi-vvodit-noviy-protokol-zadlya-dodatkovoyi-bezpeki-20180627797094

10. Інформація щодо призначення систем відеоспостереження. URL: https://www.kp.ru/guide/sistemy-bezopasnosti.html

11. Опис технології Jeweller. URL: https://electrica-shop.com.ua/articles/121.jeweller_besprovodnaya_tehnologiya_radiosvyazi

12. Датчики охоронної системи. URL: https://secur.ua/ajax

13. Порівняння технологій Інтернету речей. URL: https://controleng.ru/besprovodny-e-tehnologii/putivoditel-iot-2/

**ДОДАТОК А**

Abstract

# ABSTRACT

Security of the organization, company, office, industrial or other premises is ensured by a whole range of measures. Security systems are an important component of threat detection and neutralization. Security systems ensure the stability of the organization, performing various functions of protection and control.

Analyzing the security system should consider the types of threats it creates, as well as consider those threats that may affect the system itself. It is the security systems that can cope with the prevention of threats by providing access control to the territory of the enterprise and the protected objects, monitoring the situation in real time and taking urgent measures in case of emergencies.

The current state of the security problem is determined by many factors. The most significant of these are those that directly form the main assessments of the situation, the principles of activity of all structures in the field of security.

The analysis of a certain volume of analytical material makes it possible to draw some conclusions about the tendencies, which are created when the security systems are created. At the moment, security professionals have an interest and a willingness to take practical steps in implementing effective systems, namely:

- recognition of the need to use new elements in the structure of the system;

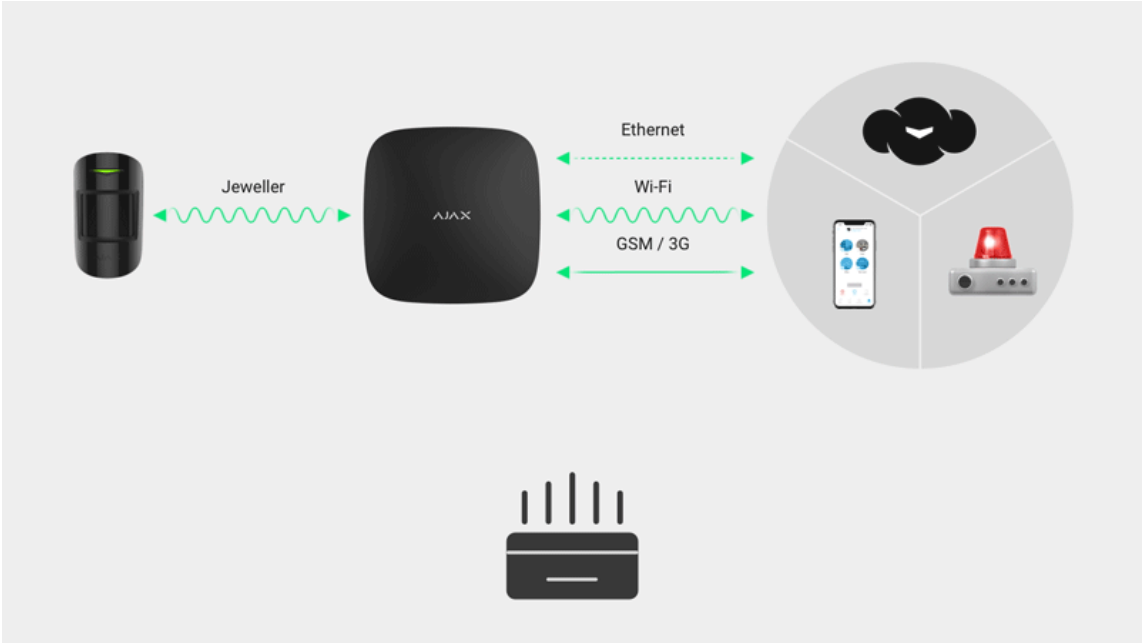
- understanding the necessity of the design stage in the construction of the system as an element of technology;

- optimization of structure and functional characteristics of the complex.

Security and access control systems ensure the security of your home or office, business, etc., both from outside penetration and from accidents indoors. Opening sensors are connected to all windows and doors. The rooms have motion sensors and camcorders. If you wish, you will always see what's happening in your home or office from anywhere in the world. This is important both when protecting your home from outsiders and when you leave your children at home with a nanny. Separately, in the house, sensors of gas leakage and water leakage are installed. When triggered, they overlap the safety valves, leaving your home unharmed.

Basic wireless technologies that address the issue of low-level IoT networks with a small area of native coverage and long-range information transmission are analyzed. A feature of multiservice networks is the presence of power at each connected object. And the problem of providing power to the sensors is very acute, complicating the use of radio technologies. To solve this problem, standards of connectivity for smart devices with high survivability and designed to minimize power consumption are used - 6LoWPAN, Bluetooth Low Energy (BLE), ZigBee, Z-Wave, EnOcean, Jeweller and more.

Jeweller is a wireless radio technology. A reliable security system requires a stable and constant connection. But high-speed and high-quality Internet is not everywhere. Therefore, AJAX alarms are designed to guarantee the security of the protected object, as well as the ability to remotely control and control the entire system, even with poor communication quality. The very compact AJAX IoT protocol allows the security system to function normally even with a GPRS Internet connection speed of 0.5 Kbps. Jeweller technology maintains the minimum required power output and saves battery power. Thanks to this, Ajax sensors are stable for up to 7 years.




Access Control Systems are an important element of the security system, both in large enterprises and in small offices. This is an effective solution to protect a building or premises from unauthorized entry. An access control and management system is a collection of various elements (equipment and components, software) that provide access

control and management to a specific object. The main function of such a decision is to manage access to a certain territory, ie to restrict it to outsiders and / or unwanted persons, as well as to identify persons who have access to the enterprise.

The advantages of Access Control Systems are obvious - their use minimizes human participation in access control, they work around the clock, allow you to keep track of working hours to maintain discipline in the company.

Information security in the broadest sense is a collection of information protection against accidental or deliberate interference. No matter what the underlying impact is: natural or artificial causes - the system owner incurs damages.

The provision and maintenance of information security includes a set of multifaceted measures that prevent, track and eliminate unauthorized access by third parties. Information security measures also aim to protect against corruption, distortion, blocking or copying of information. It is fundamentally required that all tasks be solved at the same time, but only then provides full, reliable protection.

The communication channel must be protected, using encryption and authentication technologies to ensure that the devices know whether they can trust the remote system. New cryptographic technologies, such as ECC (Elliptic Curve Cryptography), are ten times better than their predecessors. Equally important here is the management of keys to verify the reliability of the data and the reliability of the channels of their receipt. Leading have already embedded "device certificates" into most IoT devices, enabling the authentication of a wide range of devices, including cellular base stations, TVs, and more.

Encryption, authentication, and manageability are the cornerstones of robust security. There are great open source libraries that perform encryption even on IoT devices with limited computing resources. But unfortunately, most companies continue to be exposed to dangerous risks by making key management mistakes for IoT.

Device protection is first and foremost the security and integrity of code. Signing the code is required to confirm the lawfulness of its launch, and security is required during runtime so that attacks do not overwrite it at boot time. Signing the code cryptographically ensures that it has not been hacked after signing and is secure for the device. This can be

implemented at Application and Firmware levels and even on monolithic firmware devices. All critical devices, sensors, controllers or anything else should be configured to run only signed code.

In order to protect information on the Internet of Things, considerations such as communications security, security and device control should be addressed. Device protection is first and foremost the security and integrity of code. Signing the code cryptographically ensures that it has not been hacked after signing and is secure for the device. Encryption and authentication technologies are used for communication security. With regard to the encryption method, the Advanced Encryption Standard (AES) symmetric block encryption algorithm should be preferred.